Zarious @ zarious.deviantart.com

spy vs. spy

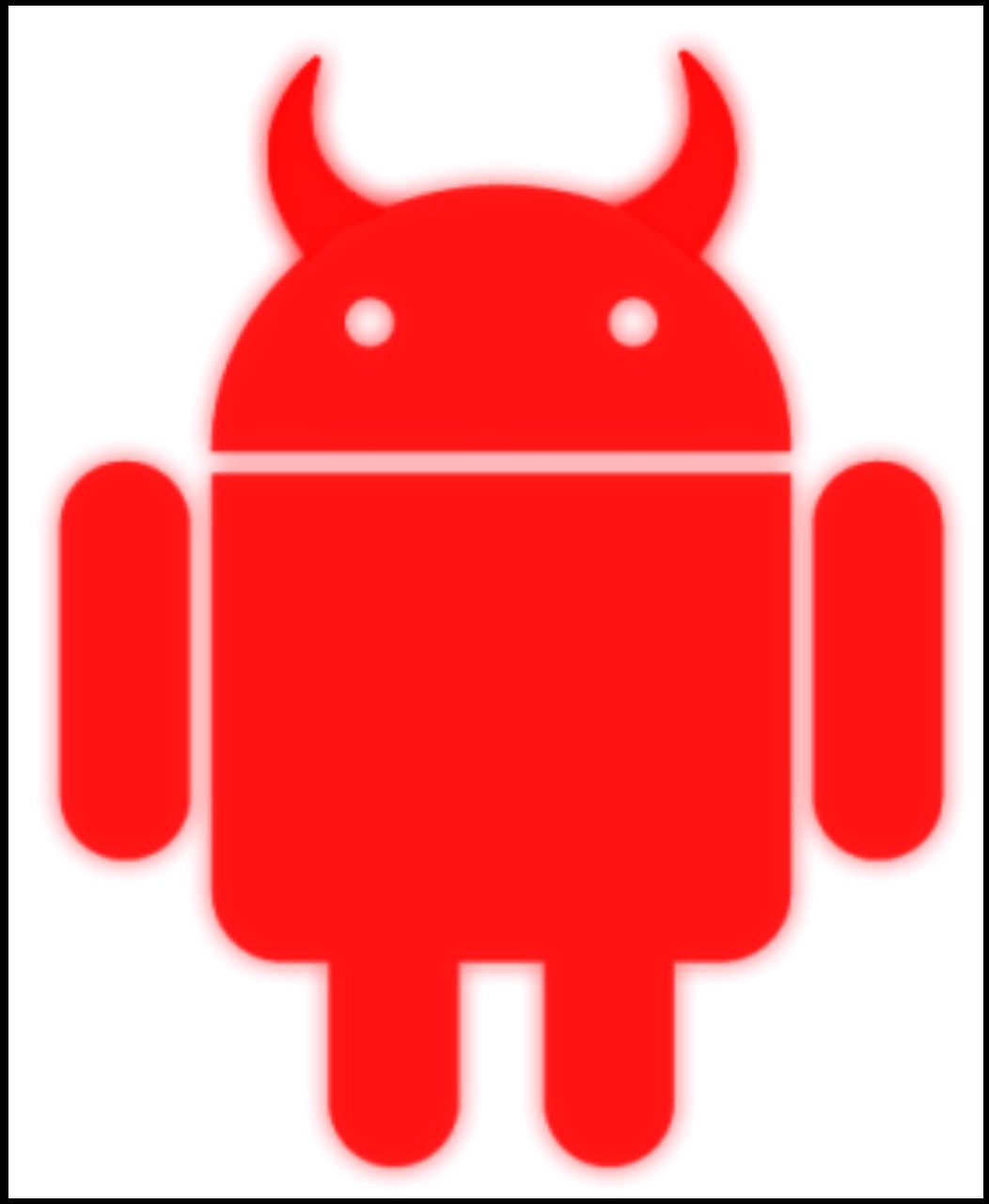
examining spyware on mobile devices

michael robinson | christopher taylor

Introduction: The newest spy

Spyware can easily run on mobile devices.

It’s in malware and its commercially available.



http://www.computerweekly.com/Articles/2011/09/12/247857/Mobile-malware-up-273-in-first-half-of-2011.htm

Mobile malware up 273% in first half of 2011

Warwick Ashford
Monday 12 September 2011 12:00

Malware for smartphones and tablets is up 273% in the first half of 2011, compared with the same period in 2010, a study has shown.

Research from G Data Security Labs shows cyber criminals are increasingly targeting mobile devices, with cross-platform Trojans dominating the malware landscape.

In the first half of 2011, researchers recorded one new malware strain every twelve seconds on average. G Data believes there is no end in sight to this malware flood.

"With mobile malware, cyber criminals have discovered a new business model," said Eddy Willems, security evangelist at G Data.

Even though this special underground market segment is still being set up, there is an enormous risk potential for mobile devices and their users, Willems said.

NickiBot Spyware
and
Zsone

NickiBot:

- Spyware (GPS monitoring, sound recording, call logs, e-mail uploading)
- Fully controlled by SMS messages
- Appears as “Android System Log” under installed applications

(See www.csc.ncsu.edu/faculty/jiang/NickiBot.)

According to Willems, researchers are expecting another spurt of growth in the mobile malware sector in the second half of the year.

Overall, G Data research shows malware is on the rise, with a new record set in the first half of 2011 of 1,245,403 new pieces of malware identified, a 15.7% increase compared to the second half of 2010.

Willems says this growth is expected to continue over the next six months and is on course to reach an annual total of new malware strains for the year of at 2.5 million, compared with just over 2 million in 2010.

SECURITY Jan 20, 2011 9:30 am

Soundminer Android Malware Listens, Then Steals, Phone Data

By Jeremy Kirk, IDG News

Researchers have developed a low-profile Trojan horse program for Google's Android mobile OS that steals data in a way that is unlikely to be detected by either a user or antivirus software.

SIMILAR ARTICLES:

Researchers Discover Android Data Leaks: What You Need to Know

Can You Trust Your Data to Google Wallet?

The malware, called Soundminer, monitors phone calls and records when a person, for example, says their credit card number or enters one on the phone's keypad, according to the study.

Using various analysis techniques, Soundminer trims the

Soundminer

- Monitors phone calls (voice and keypad)
- Sends credit card data over the network
- Paired app with another Trojan

to transmit data, intercept outgoing phone calls and access contact lists might look suspicious.

So in another version of the attack, the researchers paired Soundminer with a separate Trojan, called Deliverer, which is responsible for sending the information collected by Soundminer.

Since Android could prevent that communication between applications, the researchers investigated a stealthy way for Soundminer to communicate with Deliverer. They found what they term are several "covert channels," where changes in a feature are communicated with other interested applications, such as vibration settings.

Soundminer could code its sensitive data in a form that looks like a vibration setting but is actually the sensitive data, where Deliverer could decode it and then send it to a remote server. That covert vibration settings channel only has 87 bits of bandwidth, but that is

http://www.pcworld.com/businesscenter/article/217133/soundminer_android_malware_listens_then_steals_phone_data.html

http://slashnext.com/2011/08/mobile-malware-threats-grow-now-they-can-steal-photos-from-your-phone/

August 22, 2011 | **2 Comments**

Mobile Malware Threats Grow! Now They can Steal Photos From Your Phone.

If you're new here, you may want to subscribe to my RSS feed, Twitter and Facebook.Thanks for visiting!

Like 7 Share 27 +1 7 Tweet 210

Mobile devices are being tar
they can use to steal money
most countries. A good deal
malware tends to include stu

> *Hackers are disgui*
> *tens of thousands c*
> *Marketplace or App*
> *communications (N*
> *or Visa's payWave*

F-Secure:
Photoscraping for harassment and blackmail.

Thanks to F-Secure team we know that

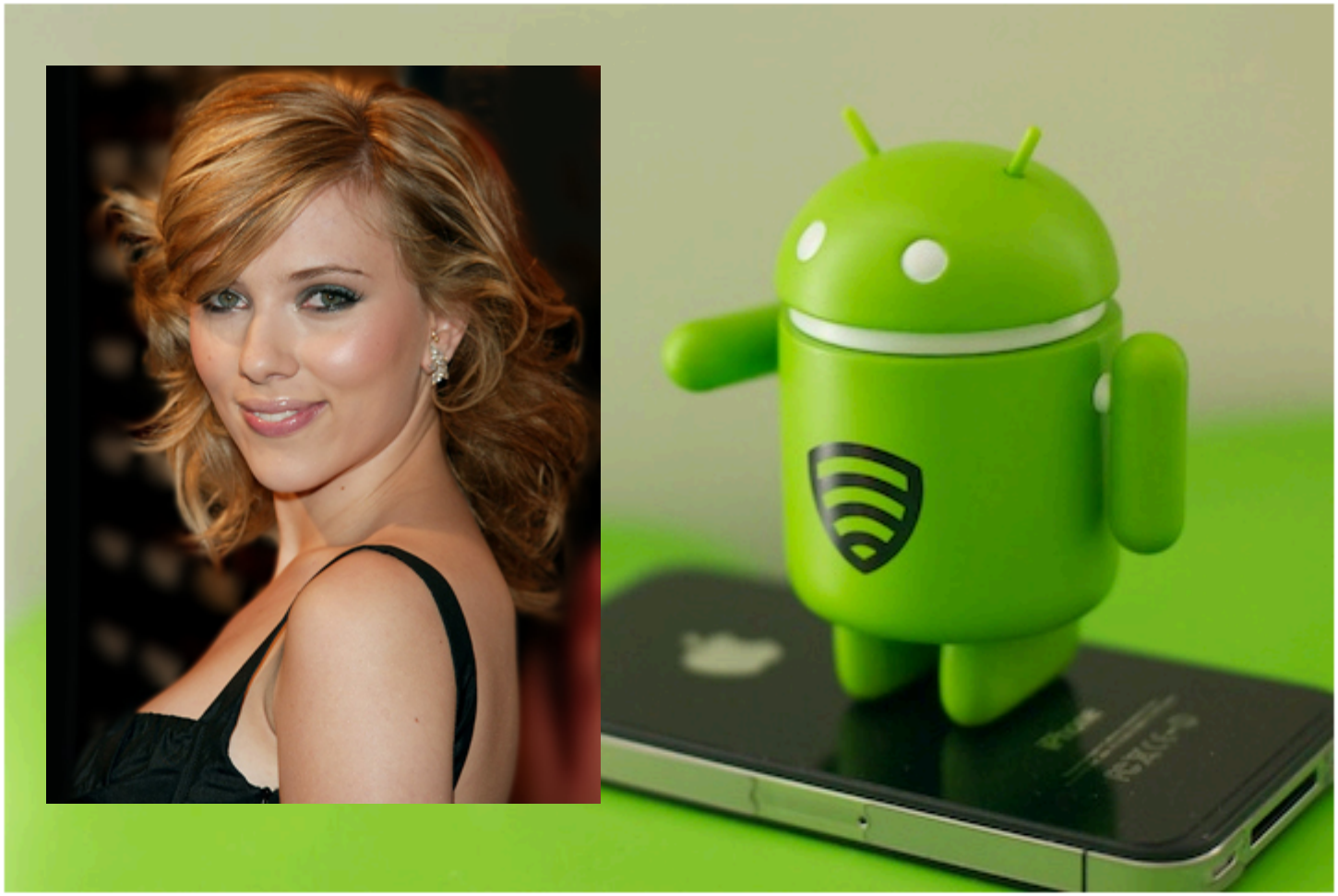
> *Chinese malware likes to spy, we've been keeping an eye out for various functions, such as photo scraping. Stealing photos from a phone could be used for harassment and blackmail. A member of Threat Response team in F-Secure just found something interesting in a Symbian malware sample.*

And what they find is very disturbing:

> *The code of Trojan:SymbOS/Spinilog.A includes a class named CMyCameraEngine which inherits and implements the Symbian class MCameraObserver. This enables the trojan to receive control when an image has been captured with the camera. Spinilog.A then encodes the raw bitmap to a JPG, which it saves to the phone's memory. This feature seems to still be unused and possibly incomplete as the*

http://www.unplggd.com/unplggd/safety-security/does-your-smartphone-need-antivirus-protection-156222

Does Your Smartphone Need Anti-Virus Protection?



After hearing about what happened to Scarlett Johansson it seems like everyone is talking about what they can do to keep the private data on their smartphone private. While it is important to follow best practices, it might be time, depending on which OS you rock on your smartphone, to consider adding an extra level of protection.

Like 3 Tweet 6 +1 0

Scarlett Johansson

Jessica Alba

Julianne Hough

Heather Morris

Miley Cirus

Mila Kunis

Olivia Munn

Ashley Greene

British Royalty

Commercialization of spyware

BlackBerry Spyware

Monitor, Trace and Track BlackBerry Smartphones

BlackBerry Spyware Spyphone Software

BlackBerry Spy technology delivers find out the specifics as to what people are saying on their **Android** as well as who they really are talking to. **Trace BlackBerry Phone Calls**, **Track BlackBerry Location**; and determine what is in **SMS texts** and **email**; find out **internet activity**; and a whole lot more. With **BlackBerry Mobile Phone Spy Software** programs you may even **cell phone tap** to **listen to smartphone calls** and **spy call** transform the smartphone right into a covert **bug device**. The BlackBerry operating system is particularly popular with mobile device software developers and normally **BlackBerry Spy** applications are packed with features unavailable with other systems; making **BlackBerry Spy** software powerful as solutions to **Parental Monitoring**, **Workforce Monitoring** and uncovering **Cheating**.

BlackBerry

Go to Phone Monitoring Websites

Compare Phone Monitoring Software

iPhone ▶ BlackBerry | android | NOKIA symbian | Windows Mobile

BlackBerry

BlackBerry Spy

Monitoring and Tracking applications is designed for most type of BlackBerrys but there are a few limitations — if you're looking to capture a history of Website Visits or Check MMS multi-media messages (images, music and video), unfortunately BlackBerry will not support keeping track of that. BlackBerry Tracker, Review SMS Texting & E-mail, Call Event Logging, Cell Phone Tap Calls and much more.

Go to Phone Monitoring Websites

Compare Phone Monitoring Software

Go To MOBILE·SPY

Go To PHONESHERIFF

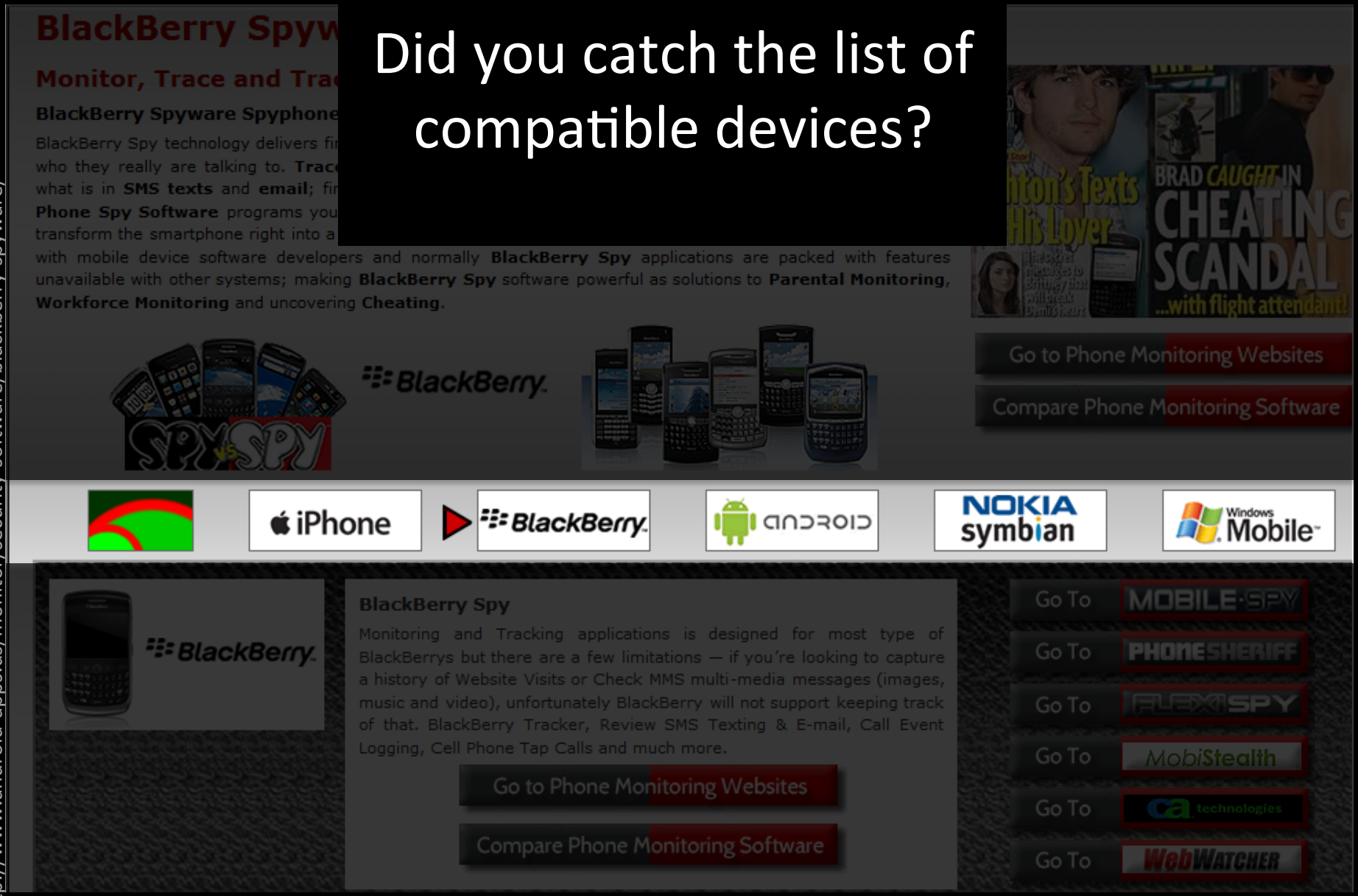
Go To FLEXISPY

Go To MobiStealth

Go To ca technologies

Go To WebWatcher

Did you catch the list of compatible devices?



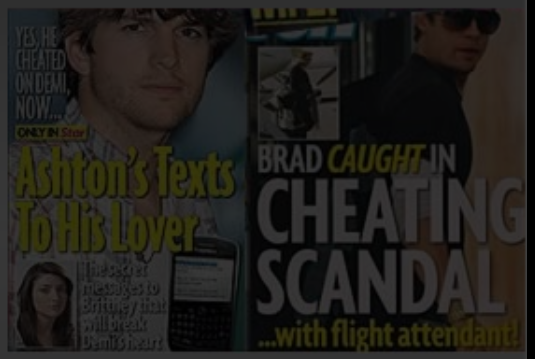
http://www.android-apps.us/monitor/security-software/blackberry-spyware/

BlackBerry Spyware

Monitor, Trace and Track BlackBerry Smartphones

BlackBerry Spyware Spyphone Software

BlackBerry Spy technology delivers find out the specifics as to what people are saying on their **Android** as well as who they really are talking to. **Trace BlackBerry Phone Calls**, **Track BlackBerry Location**; and determine what is in **SMS texts** and **email**; find ... **Mobile Phone Spy Software** programs you n... **call** transform the smartphone right into a c... popular with mobile device software developer... tures unavailable with other systems; making ... **ring**, **Workforce Monitoring** and uncovering ...



Go to Phone Monitoring Websites

Compare Phone Monitoring Software

iPhone · Black... · android · NOKIA symbian · Windows Mobile

And this is the short list.

BlackBerry

BlackBerry Spy

Monitoring and Tracking ... is designed for most type of BlackBerrys but there are a... ions — if you're looking to c... ure a history of Website Visits o... music and video), unfortunat... of that. BlackBerry Tracker, ... Logging, Cell Phone Tap Calls and ...

Go to Phone Monitoring Websites

Compare Phone Monitoring Software

Go To MOBILE·SPY

Go To PHONESHERIFF

Go To FLEXISPY

Go To MobiStealth

Go To ca technologies

Go To WebWatcher

http://www.android-apps.us/monitor/security-software/blackberry-spyware/

Some commercial versions
don’t require rooting of the phone.*

* iPhones need to be jailbroken.

So what does it do?

Commercial spyware may capture:

- SMS activity
- Location/GPS coordinates
- Pictures
- Videos
- Inbound/outbound call logs
- Browser activity (URLs)
- E-mail
- Identify SIM card changes

Interactive mode may include:

Taking pictures

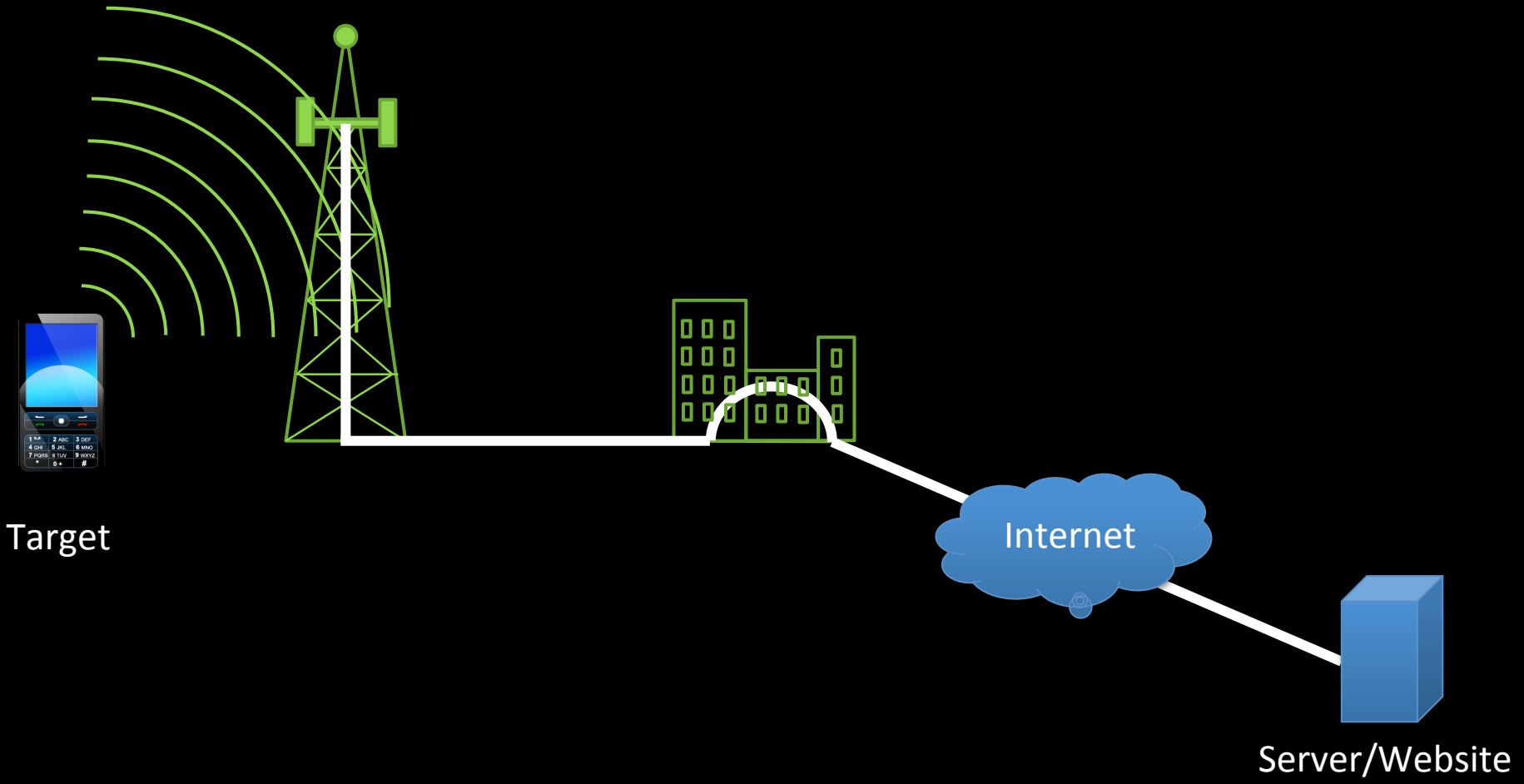
Recording videos

Record conversations/background via calls

Wiping the phone

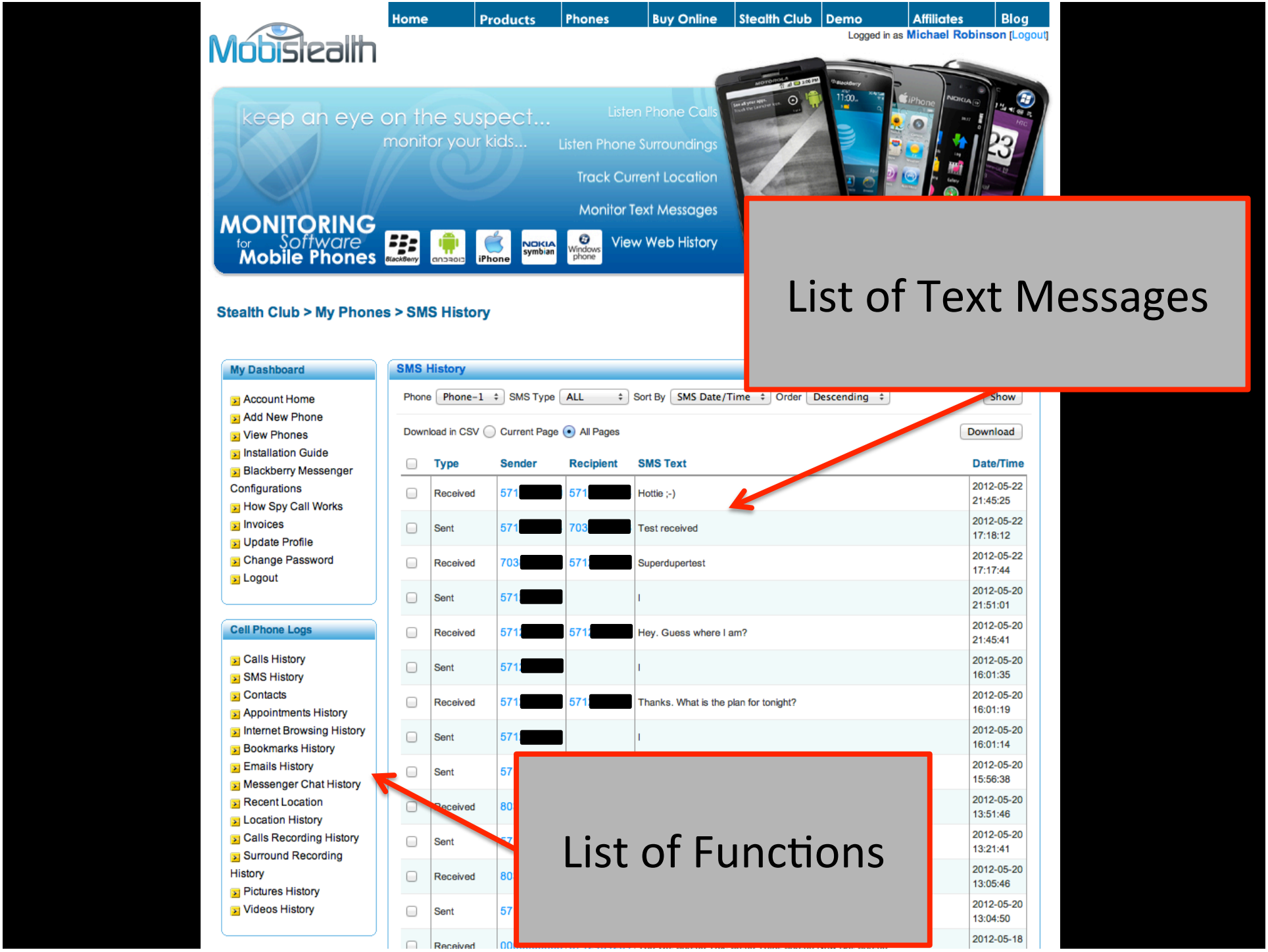
Viewing the target phone's screen

Harvested data sent back to a server.



For example:


English
SpyBubble
Truth Exposed
HOME
CALLS
SMS
GPS
PHOTO
URLS
PHONE
LOGOUT
Call Details !!!
Calls From : 05/23/2012
Calls To : 05/23/2012
Call Type : All
Keyword :
Search
Serial No
Time of Call
Phone Number
Type Of Call
Duration
1 2012-05-23 04:24:22 *999999# Outgoing 00:00:00
2 2012-05-23 04:23:48 *999999# Outgoing 00:00:04
3 2012-05-22 17:37:43 999999 Outgoing 00:00:00
4 2012-05-22 17:18:35 571[redacted] Outgoing 00:00:26
5 2012-05-22 17:14:26 571[redacted] Outgoing 00:00:11
6 2012-05-22 17:13:38 *999999# Outgoing 00:00:18
Delete Selected
Download CSV
Displaying 1 to 6 (of 6 Records)
Log Viewers
Account Summary
Call Details
SMS Details
GPS Details
Url Details
Cell Location
Photo Details
Phonebook
Calendar Details
Call Recordings Details
Environment Recordings
Live Pictures
Live Videos
Live Functionalities
Settings
Change Password
Logout
Any Question?
List of Functions
Call records


Home
Products
Phones
Buy Online
Stealth Club
Demo
Affiliates
Blog
Logged in as Michael Robinson [Logout]
keep an eye on the suspect...
monitor your kids...
Listen Phone Calls
Listen Phone Surroundings
Track Current Location
Monitor Text Messages
View Web History
MONITORING for Software Mobile Phones
Stealth Club > My Phones > SMS History
My Dashboard
Account Home
Add New Phone
View Phones
Installation Guide
Blackberry Messenger Configurations
How Spy Call Works
Invoices
Update Profile
Change Password
Logout
Cell Phone Logs
Calls History
SMS History
Contacts
Appointments History
Internet Browsing History
Bookmarks History
Emails History
Messenger Chat History
Recent Location
Location History
Calls Recording History
Surround Recording History
Pictures History
Videos History
SMS History
Phone Phone-1 SMS Type ALL Sort By SMS Date/Time Order Descending Show
Download in CSV Current Page All Pages Download
Type Sender Recipient SMS Text Date/Time
Received Hottie ;-) 2012-05-22 21:45:25
Sent Test received 2012-05-22 17:18:12
Received Superdupertest 2012-05-22 17:17:44
Sent I 2012-05-20 21:51:01
Received Hey. Guess where I am? 2012-05-20 21:45:41
Sent I 2012-05-20 16:01:35
Received Thanks. What is the plan for tonight? 2012-05-20 16:01:19
Sent I 2012-05-20 16:01:14
2012-05-20 15:56:38
2012-05-20 13:51:46
2012-05-20 13:21:41
2012-05-20 13:05:46
2012-05-20 13:04:50
2012-05-18
List of Text Messages
List of Functions


English
SpyBubble
Truth Exposed
HOME
CALLS
SMS
GPS
PHOTO
URLS
PHONE
LOGOUT
Live Photos Details
From :
05/23/2012
To :
05/23/2012
Search
lp-1337672867.jpg
2012-05-22
00:47:42
lp-1337648244.jpg
2012-05-21
17:57:02
Delete Selected
Displaying 1 to 1 (of 2 Records)
Anti Theft for Mobile with Secure Data Backup and Remote Wipe
Download Now
Log Viewers
Account Summary
Call Details
SMS Details
GPS Details
Url Details
Cell Location
Any Question?
Live pictures

My Dashboard

- Account Home
- Add New Phone
- View Phones
- Installation Guide
- Blackberry Messenger Configurations
- How Spy Call Works
- Invoices
- Update Profile
- Change Password
- Logout

Cell Phone Logs

- Calls History
- SMS History
- Contacts
- Appointments History
- Internet Browsing History
- Bookmarks History
- Emails History
- Messenger Chat History
- Recent Location
- Location History
- Calls Recording History
- Surround Recording History
- Pictures History
- Videos History

Computer Logs

- Access Tracker
- Bookmarks History
- Emails History
- Internet Browsing History
- Keystroke Logs
- Location History
- MSN Chat History
- Screenshot History
- Skype Call Recording
- Skype Chat History
- Surround Recording History
- YAHOO Chat History

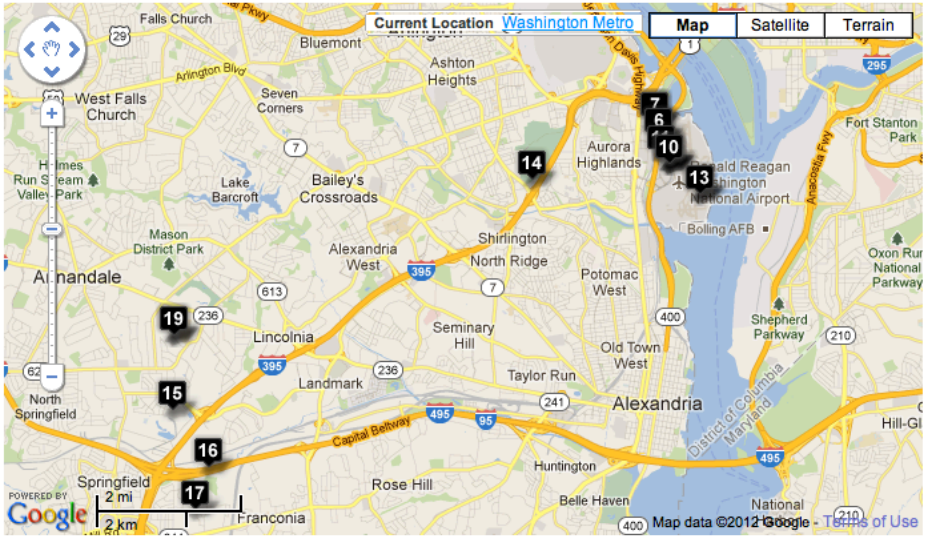
Settings

Location History

Phone: Phone-1 | Starting From: 2012-05-19 | Ends On: 2012-05-22 | Show

Show empty/unavailable location records

Download in CSV: Current Page / All Pages | Download



To get the address of a location, click the certain marker on above map.

		Date	Phone	Latitude	Longitude
☐	1	2012-05-20 21:55:43	571[redacted]	36.08569444444444	-115.14902777777777
☐	2	2012-05-20 21:47:43	571[redacted]	36.08569444444444	-115.14902777777777
☐	3	2012-05-20 16:17:28	571[redacted]	38.85923611111111	-77.04930555555555
☐	4	2012-05-20 16:09:27	571[redacted]	[illegible]	[illegible]
☐	5	2012-05-20 16:01:28	571[redacted]		
☐	6	2012-05-20 15:53:27	571[redacted]		
☐	7	2012-05-20 15:45:27	571[redacted]		
☐	8	2012-05-20 15:37:26	571[redacted]		
☐	9	2012-05-20 15:29:26	571[redacted]		
☐	10	2012-05-20 15:21:26	571[redacted]		
☐	11	2012-05-20 15:13:26	571[redacted]		
☐	12	2012-05-20 15:05:24	571[redacted]		
☐	13	2012-05-20 14:57:25	571[redacted]		
☐	14	2012-05-20 14:49:23	571[redacted]		
☐	15	2012-05-20 14:41:23	571[redacted]		
☐	16	2012-05-20 14:33:23	571[redacted]	38.801180555555554	-77.17333333333333

GPS Coordinates
(Actually cell phone towers)

My Dashboard

- Account Home
- Add New Phone
- View Phones
- Installation Guide
- Blackberry Messenger Configurations
- How Spy Call Works
- Invoices
- Update Profile
- Change Password
- Logout

Cell Phone Logs

- Calls History
- SMS History
- Contacts
- Appointments History
- Internet Browsing History
- Bookmarks History
- Emails History
- Messenger Chat History
- Recent Location
- Location History
- Calls Recording History
- Surround Recording History
- Pictures History
- Videos History

Calls Recording History

Phone: Phone-1 | Observed Number: ALL | Sort By: Stealth Date/Time | Order: Descending | Show

Select All / Deselect All

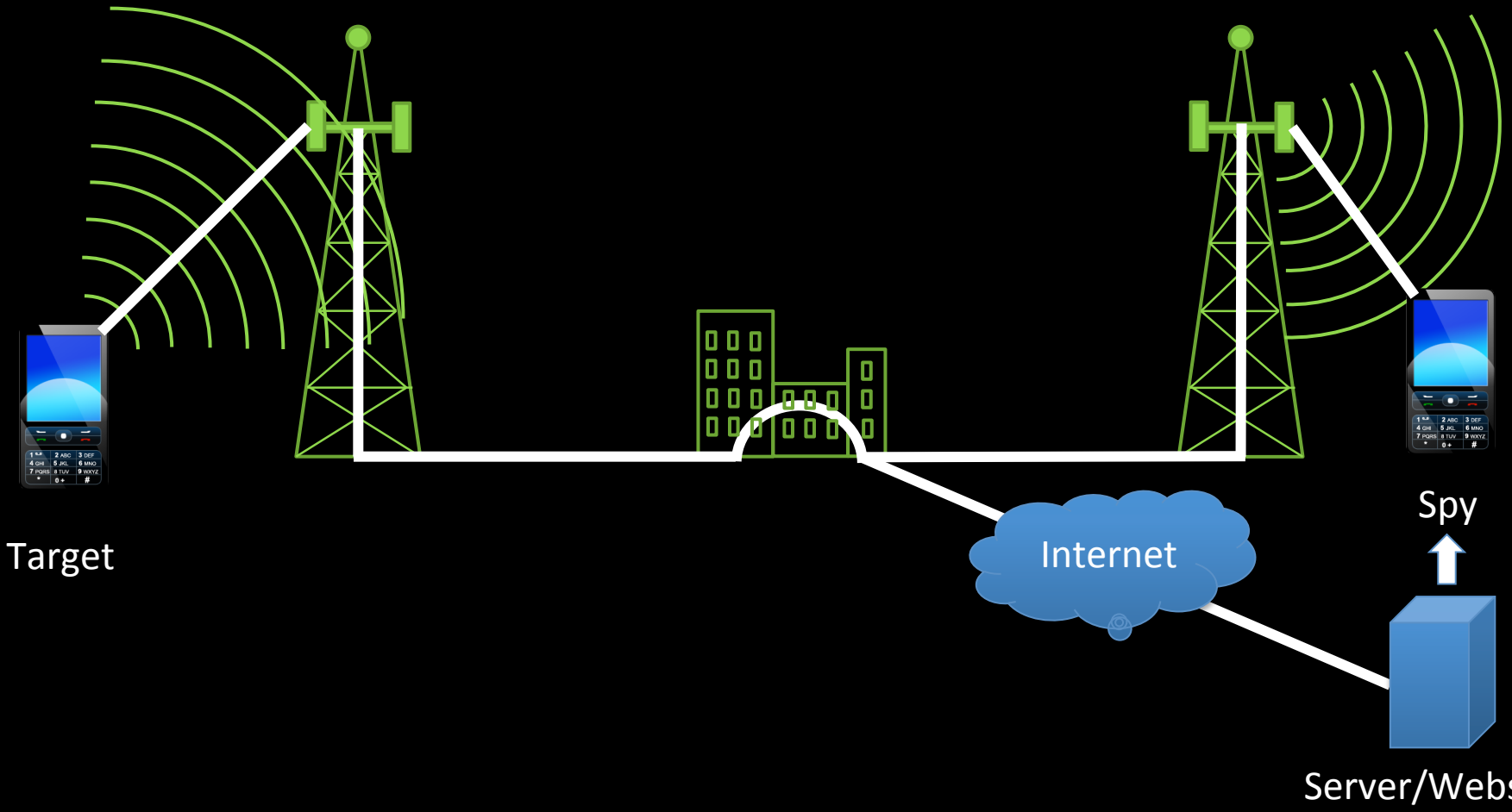
Number: 7038[redacted] 2012-05-22 17:19:06	Number: 703[redacted] 2012-05-21 17:59:16	Number: 571[redacted] 2012-05-20 15:53:38	Number: 410[redacted] 2012-05-20 13:44:06
Number: 410[redacted] 2012-05-20 13:40:32			

Delete Selected | Download Selected

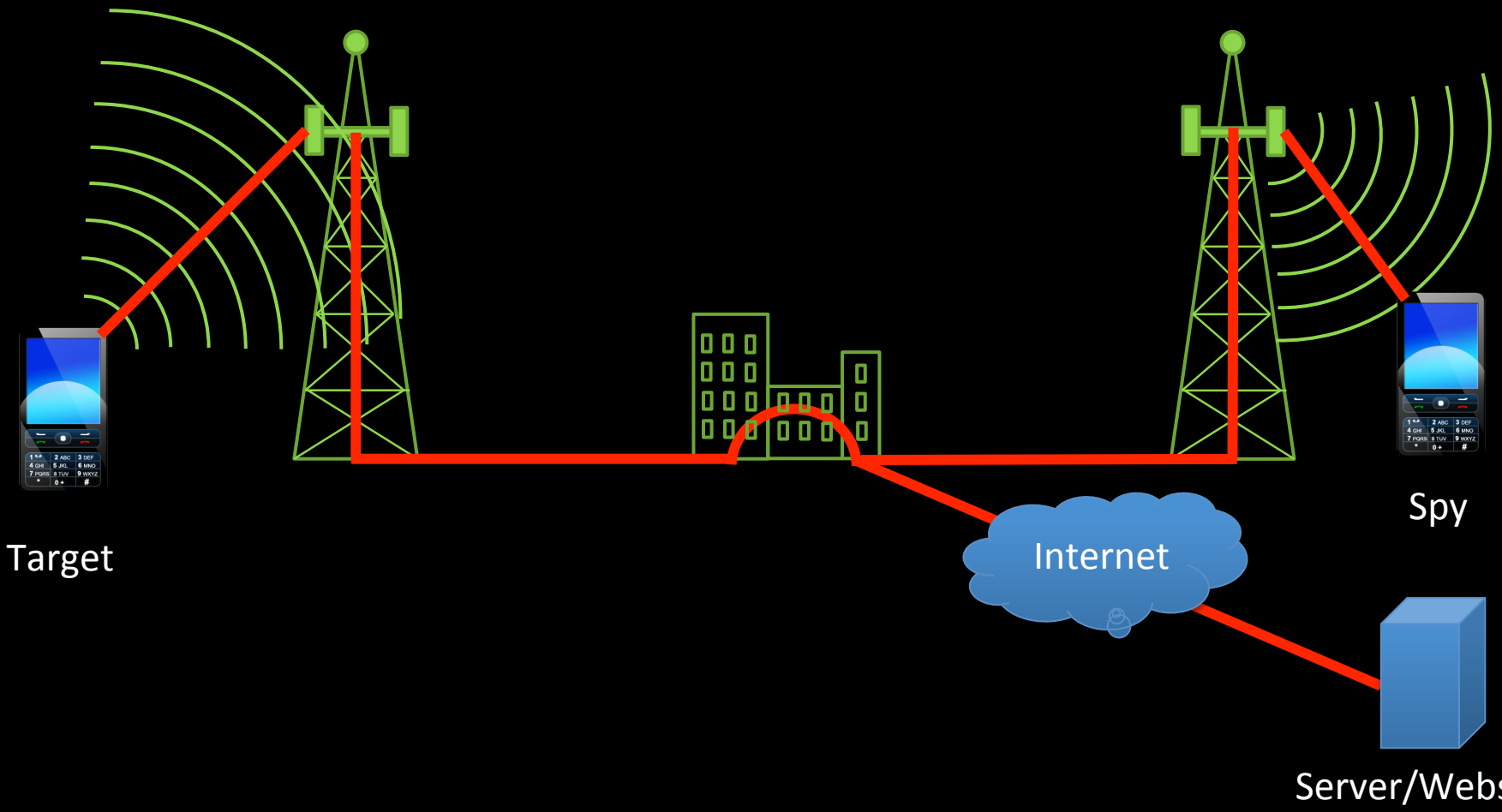
How to play these recordings?

Recorded phone calls

Alerts can be sent to a monitoring phone via SMS directly from target or from the website.



Commands can be sent to the target phone via the observing phone or website.



Principle differences between malware and commercial versions:

Attack vector
(delivery method)

Logging

Installation

- Physical access: required.
- Android rooting: not always required.
- iPhone Jailbreaking: required.
- Internet connection: required.
- Ability to install apps from unknown sources.: required
- Device may need to be rebooted.

The BIG question:

How do you know if you've been PWN'd?

You wouldn't know, would you? Spyware is "undetectable."

Q: Will other people know that SpyBubble is installed or running on the mobiles I provide them with?
A: No, there is no icon or symbol that shows the status of SpyBubble on the screen of the mobile.

Will users know MobiStealth is installed or running?

MobiStealth uses the latest innovations in mobile monitoring to keep your monitoring safe and secure. There are no indications that MobiStealth is running while it is active. It runs in completely stealth mode.

Will users know Mobile Spy is installed or running?
Mobile Spy uses the latest innovations in mobile monitoring to keep your monitoring safe and secure. There are no indications that Mobile Spy is running while it is active. The program has no entries in the User Menu, and its files are extremely discreet. Best of all, when Mobile Spy is running, there is **NO** entry for it in the Task Manager. So it is your responsibility to notify any user they are being monitored.

Here’s what we did:

We forensically examined smart phones infected with different commercial spyware products.

HTC Wildfire S (rooted)
on T-Mobile

FLEXISPY

LG Optimus Elite
on Virgin Mobile

SpyBubble
La Verdad Al Descubierto

LG Optimus V
on Virgin Mobile

Mobistealth

Samsumg Galaxy Prevail
on Boost/Sprint

MOBILE·SPY
SPY SOFTWARE FOR SMARTPHONES

Apple iPhones 4s (jailbroken)
on T-Mobile

spyera
The Best Spyphone Software

the legal stuff

FLEXISPY™
Revealing Secrets Since 2005

English

Call Us!
USA: (1) 646-240-4063
UK: (44) 207-979-7126

Live Support
ONLINE

PRODUCTS | SUPPORT | QUICK BUY | LEARN MORE | ABOUT US | RESELLERS

Legal Disclaimer

LEGAL DISCLAIMER

Get the facts and understand your liability

Flexispy Ltd. Full Legal Disclaimer

Updated 2011

In some areas it may be a Federal or State offense to install software onto a phone you do not own, without the owners awareness & consent. We do not condone the use of our software for any illegal purpose. By purchasing, download or using our software in any way, form or fashion, you acknowledge & approve the following:

1. You represent that FlexiSPY will be used exclusively in a lawful manner. If you're in doubt as to the legality of your planned usage we require you consult with a registered attorney for the jurisdiction where you intend to use FlexiSPY.
2. You acknowledge you own the mobile phone you will install the software on, or have consent from the owner to administrate the device & install software onto it.
3. FlexiSPY ltd will never release any of your private information or account data for any reason whatsoever, EXCEPT under threat of legal action or court order. If you use our software to commit a crime & a warrant or subpoena for records is issued by court order as part of an ongoing investigation, we are legally bound to comply. This may include the release of purchase information or other customer data as ordered by a judge.
4. You acknowledge that you are solely responsible for how you use the software, & for complying with all relevant laws in your area. You also acknowledge that neither FlexiSPY ltd, nor any of its agents, affiliates, directors, employees & associates may be held liable, responsible or accountable for any type of damage, litigation or other legal action, which may arise either from your legal or illegal use of FlexiSPY software, websites, or any other software & under no circumstances will you be eligible for any form of compensation from the aforementioned.

the legal stuff

MobiStealth

End User License Agreement

End User License Agreement (EULA)

It may be a federal and/or state offense to install monitoring/surveillance software onto a Phone/Computer which **you do not own** or have proper authorization to install. It may also be an offense in your jurisdiction to monitor the activities of other individuals. Check all state, federal and local laws before installing any Monitoring Software such as Mobistealth. You may also have to notify a person that they are being monitored **if they are over age 18**. Federal or local law governs the use of some types of software; it is responsibility of the user to follow such laws."

The Computer Fraud and Abuse Act ("CFAA", 18 U.S.C. § 1030)

In Section 1030(g), CFAA provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. 1030(g). CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." Id. at § 1030(e)(8). CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." *Id.* at § 1030(e)(11).

"It is the responsibility of the service user to determine, and obey, all applicable laws in their country and/or local jurisdiction regarding the use of the software and services. The software and service is intended to provide the Licensee with the ability to capture, store and control their own access to information.
installing Mobistealth, you represent that Mobistealth will be used in only a lawful manner. Logging other people's Cell Phone or Computer data or installing Mobistealth on another person's Phone/Computer without their knowledge can be considered as an illegal activity in your country. Mobistealth assumes no liability and is not responsible for any misuse or damage. It is the final user's responsibility to obey all laws in their country and/or State
Regardless of the state, it is almost always illegal to record a conversation to which you are not a party, do not have consent to tape, and could not naturally overhear. Federal law and most state laws also make it illegal to disclose the contents of an illegally intercepted call or communication.
Federal law and most state laws also make it illegal to disclose the contents of an illegally intercepted call or communication.
We do not manage the data, nor control distribution of data, nor access personal data captured or stored on servers and databases we provide. We cannot, and have no responsibility to, access, recover, retrieve or read any data or information captured by Licensee or other party use of the software and service. The publisher and vendor make no warranty, assume no liability, and are not responsible in any way for any misuse or damage caused by using the software or services. The software user must accept all risk and liability for use. Use of the software and service constitutes acceptance of these terms & conditions and grants indemnification of the software supplier. All trademark, copyright images and wordmarks displayed on this website are property of their respective owners.

Refund Policy

1. If there is any issue with functionality of MobiStealth on your Phone/Computer then we shall work with you to resolve the issue. If issue cannot be resolved only then a refund will be issued. Customer is required to report the issue within 10 days of purchasing MobiStealth.
2. Customer bears the responsibility of installation of software on the target Phone/Computer that needs to be monitored. In the event a purchase is made under the false assumption that physical access is not needed to install the software on the target/monitored Phone/Computer, Mobistealth is not liable to issue any refund.

the legal stuff

Disclaimer: SpyBubble is a Mobile Phone Spy Software, basically designed for monitoring your spouse, children or employees having Smartphone. Either you should own the phone or you should have permission to monitor from the user of smartphone.

If you fail to comply, depending on federal and state laws, you could be breaking the law. The SpyBubble will allow you to monitor Mobile phones as a tool NOT for illegal purposes. Use only at your discretion. The use of the software is done at your own discretion and risk and with agreement that you will be solely responsible for any damage to your Mobile or loss of data that results from such activities. No advice or information, whether oral or written, obtained by you from us or from the SpyBubble web site shall create any warranty for the software. In addition, you agree to hold harmless the publisher and authors personally and collectively for any losses of relationships, capital (if any) that may result from the use of this application. Your use of SpyBubble like other software agreements, indicates your acceptance of these disclaimers.

NOTE : All trademarks on this site are property of their respective owners. These companies are not affiliated with SpyBubble.com in any way. Mentioned trademarks are used solely for the purpose of describing phone and carrier compatibility for our mobile phone spy software.

the legal stuff

User Legal Agreement

Information regarding our products and services.

All users are required to accept these terms as well as the terms located on the Legal Information page when creating your account and upon purchase.

It is a federal and state offense to install surveillance software onto a device which you do not have proper authorization.

We absolutely do not condone the use of our software for illegal purposes.
In order to purchase our software you MUST agree to the following conditions.

1. You acknowledge and agree that you own the device you will install the software onto OR that you have the expressed written consent of the owner to be an authorized administrator of the device and its users.

2. If you install our software onto a phone which you do not own or have proper consent, we will cooperate with law officials to the fullest extent possible. This includes turning over requested customer data, and any other purchase/product related information.

3. You agree that you will check all local, state and federal laws to make sure you are complying with all laws in your region. It may be illegal in your region to monitor other individuals on your own device. You will never monitor any adult without their valid permission.

4. You agree to the conditions in our EULA (End-User License Agreement). This includes the fact that we are not liable for any type of damage, litigation, or legal predicaments that may arise due to use or abuse of Mobile Spy or any other product.

5. All logs are subject to deletion after thirty (30) days for maintenance purposes.

the legal stuff

End User License Agreement

NOTICE TO USER: PLEASE READ THIS CONTRACT CAREFULLY. BY USING ALL OR ANY PORTION OF THE SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT

1. The user hereby undertakes to use the software responsibly and obey all applicable laws in which ever jurisdiction the software is operating.

2. The user understands that the Server side data is held for the purposes of downloading to their own systems and that this should be done on a regular basis and at least every seven (7) days. If data is not downloaded within this period Spyera reserve the right to permanently delete it.

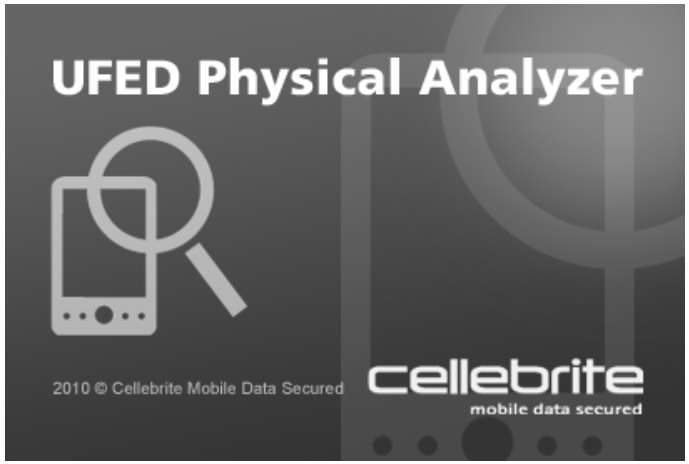
3. The user explicitly indemnifies Spyera for any harm financial or by reputation that may arise as a result of the misuse of this software.

4. Intellectual Property Rights. The Software and any copies that you are authorized by Spyera to make are the intellectual property of and are owned by Spyera Software LLC (Hong Kong). The Software is protected by copyright, including without limitation by international treaty provisions and applicable laws in the country in which it is being used. You may not copy the Software, you may however transfer the license from one phone to another providing the original device is first deactivated. You agree not to modify, adapt or translate the Software. You also agree not to reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software without the express written permission of Spyera . This Agreement does not grant you any intellectual property rights in the Software.

5. Transfer. You may not rent, lease, sublicense or authorize all or any portion of the Software to be copied onto another users phone except as may be expressly permitted herein. You may, however, transfer all your rights to use the Software to another person or legal entity provided that:
(a) you also transfer this Agreement to such person or entity;
(b) you retain no copies, including backups and copies stored on a computer; and
(c) the receiving party accepts the terms and conditions of this Agreement and any other terms and conditions upon which you legally purchased a license to the Software.

6. It is the responsibility of the user of Spyera to ascertain, and obey, all applicable laws in their country in regard to the use of Spyera for "sneaky purposes". If you are in doubt, consult your local attorney before using Spyera. By downloading and installing Spyera, you represent that Spyera will be used in only a lawful manner. Logging other people's SMS messages & other phone activity or installing Spyera on another person's phone without their knowledge can be considered as an illegal activity in your country. Spyera assumes no liability and is not responsible for any misuse or damage caused by our Software. It's final user's responsibility to obey all laws in their country. By purchasing & downloading Spyera, you hereby agree to the above.

Forensic Tools




SPY
FLEXISPY

URL history

Title: FlexiSPY Product Download

URL: http://djp.cc

Cookie

Name: JSESSIONID

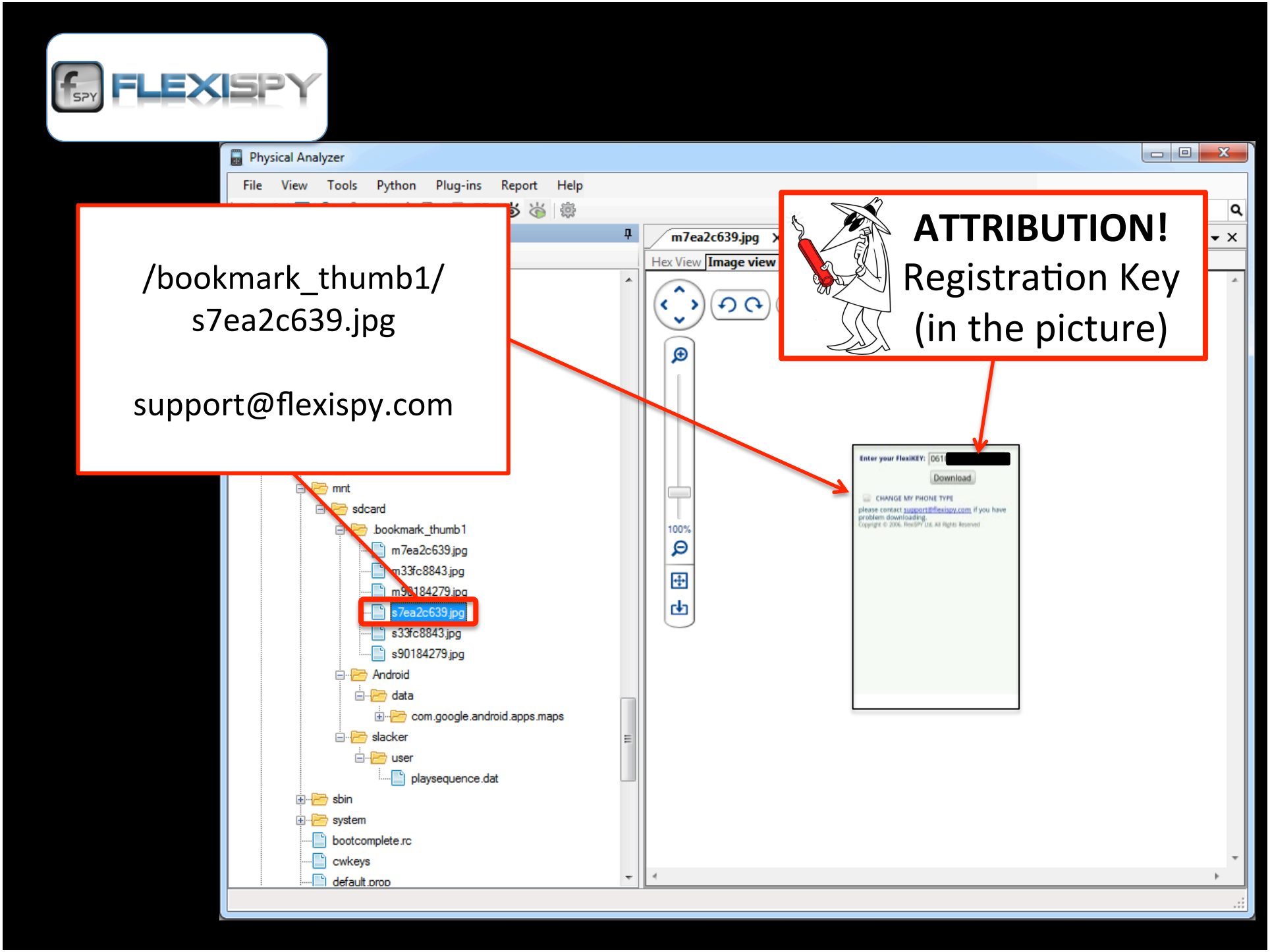
Domain: djp.cc

Search of physical dump

http://djp.cc/checkkey?key=[redacted]&
Submit=Download.FSXGAD_2.03.3.apk/mnt/sdcard/download/
FSXGAD_2.03.3.apkapplication/vnd.android.package-archive

SD Card

\download\FSXGAD_2.03.3.apk

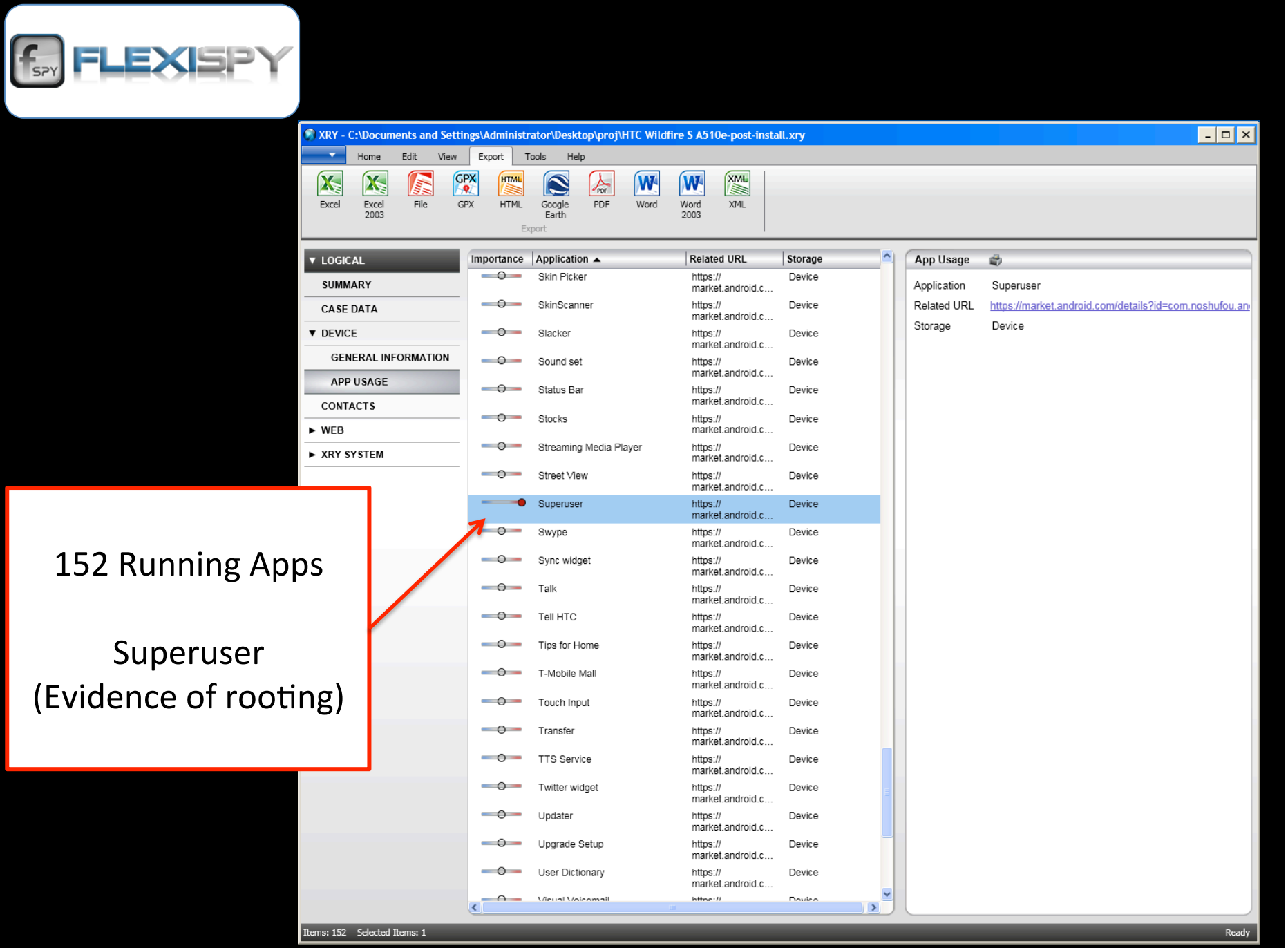

FLEXISPY
Physical Analyzer
File View Tools Python Plug-ins Report Help
/bookmark_thumb1/
s7ea2c639.jpg
support@flexispy.com
ATTRIBUTION!
Registration Key
(in the picture)
m7ea2c639.jpg
Hex View
Image view
100%
mnt
sdcard
bookmark_thumb1
m7ea2c639.jpg
m33fc8843.jpg
m90184279.jpg
s7ea2c639.jpg
s33fc8843.jpg
s90184279.jpg
Android
data
com.google.android.apps.maps
slacker
user
playsequence.dat
sbin
system
bootcomplete.rc
cwkeys
default.prop
Download

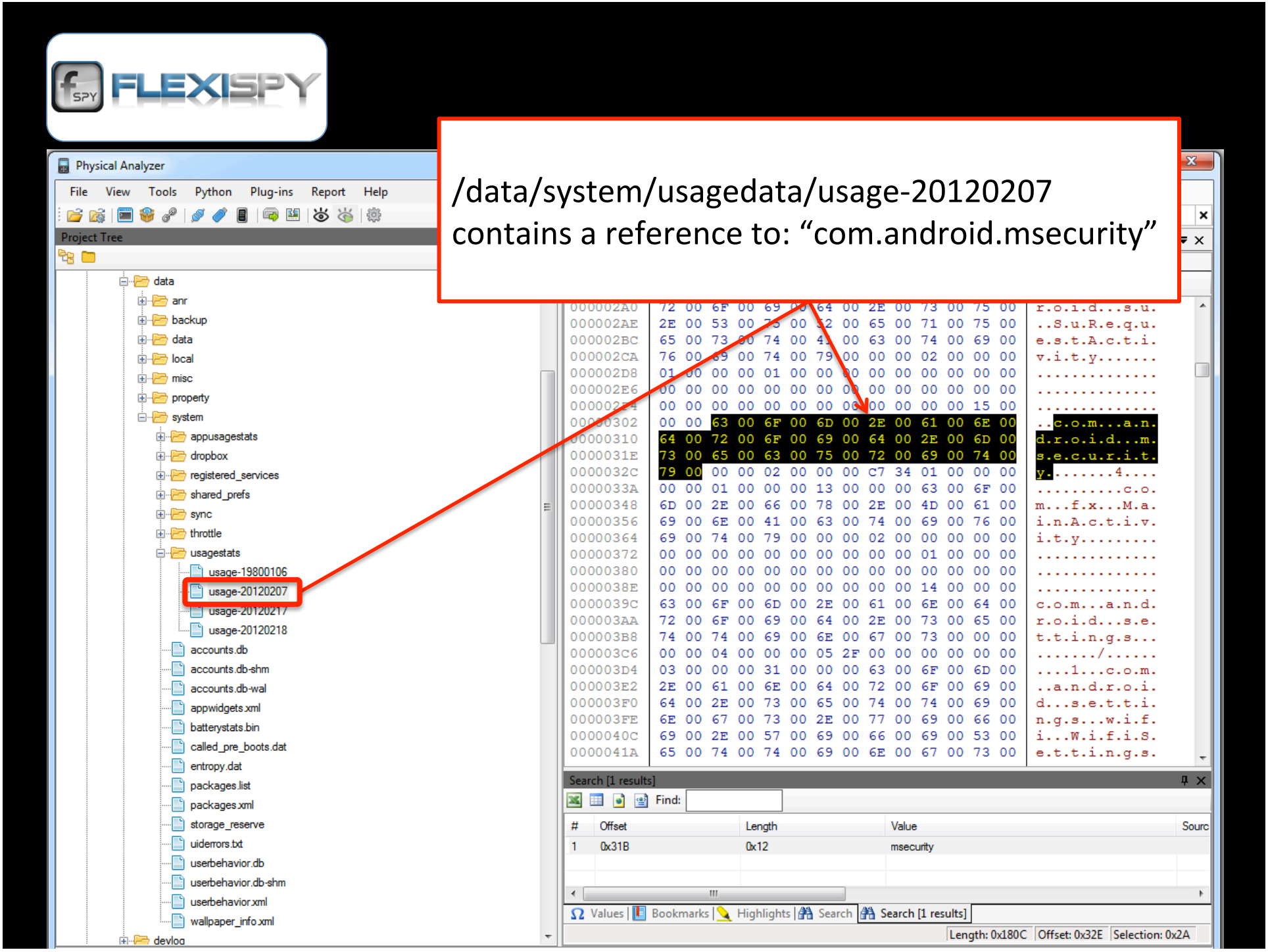
A couple of glitches…

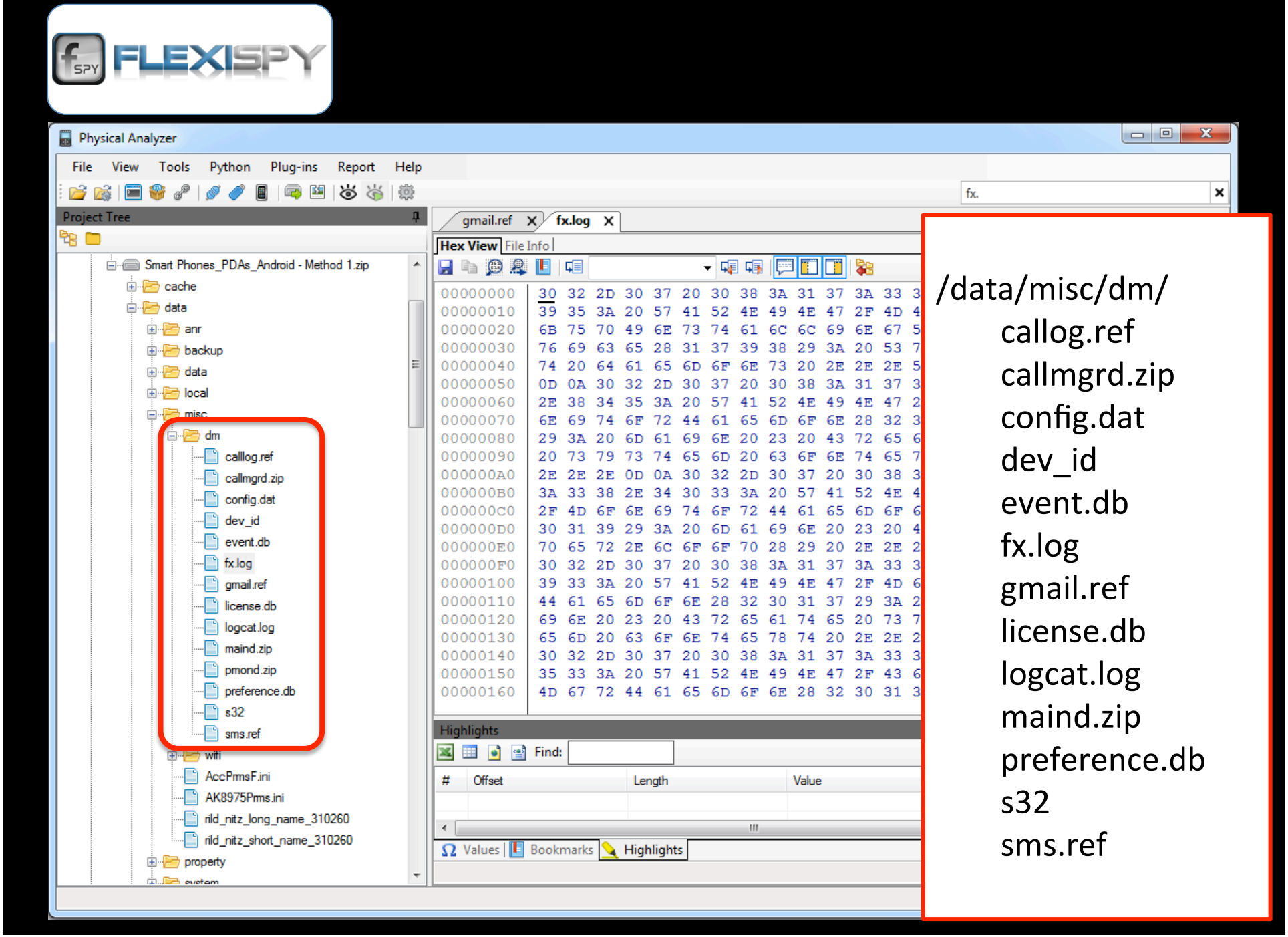
On the version we tested, we noticed:

- Messages appeared periodically that "unknown" obtained "superuser access."
- The software didn't always launch on reboot.
- On CDMA phones, stealthy messages sent to the target phone appeared to the user, i.e., they were not stealthy.
- Stealthy phone calls did not work on CDMA phones.

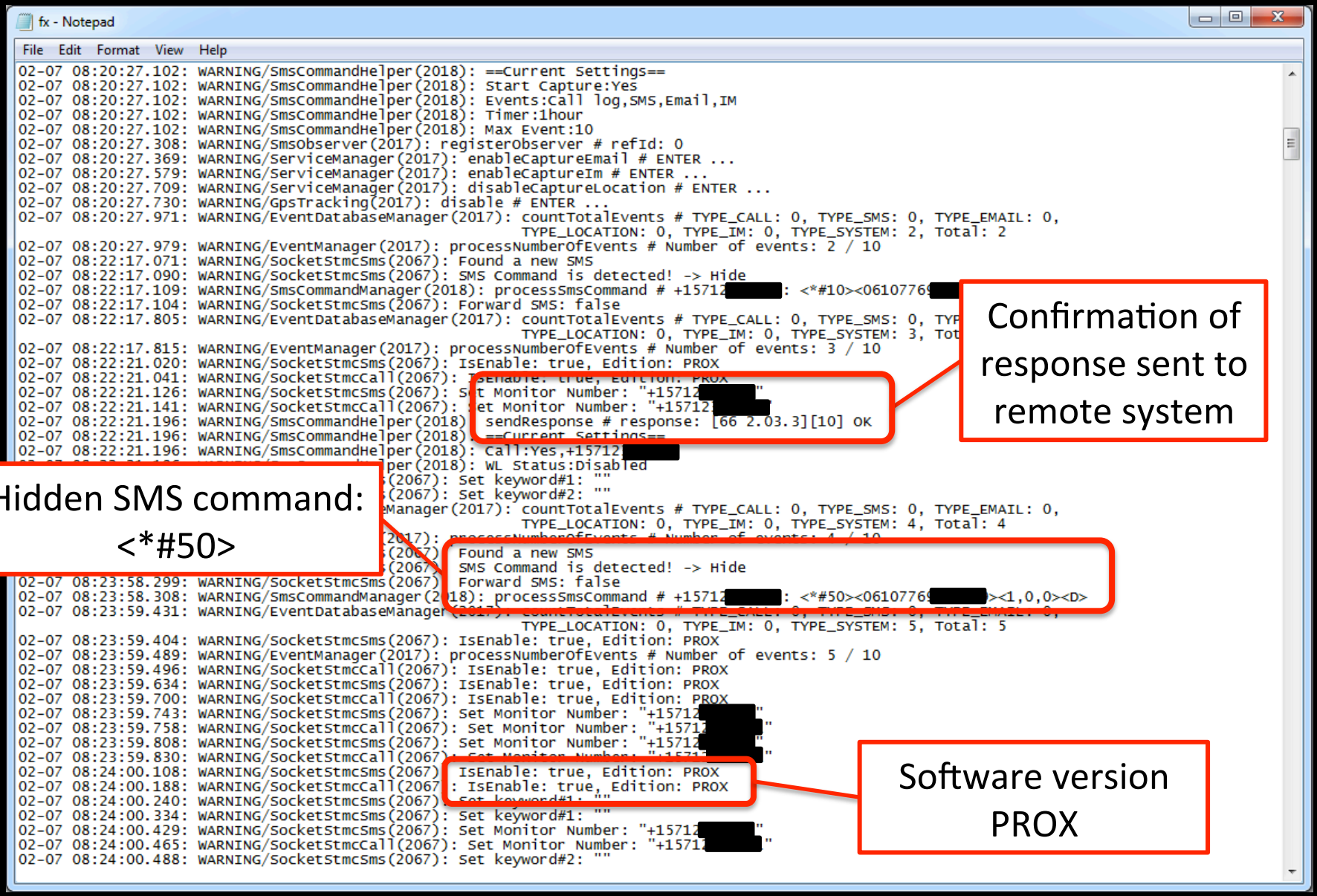
Note: A new version of the product has since been released.


FLEXISPY
XRY - C:\Documents and Settings\Administrator\Desktop\proj\HTC Wildfire S A510e-post-install.xry
Home
Edit
View
Export
Tools
Help
Excel
Excel 2003
File
GPX
HTML
Google Earth
PDF
Word
Word 2003
XML
Export
LOGICAL
SUMMARY
CASE DATA
DEVICE
GENERAL INFORMATION
APP USAGE
CONTACTS
WEB
XRY SYSTEM
Importance
Application
Related URL
Storage
Skin Picker
SkinScanner
Slacker
Sound set
Status Bar
Stocks
Streaming Media Player
Street View
Superuser
Swype
Sync widget
Talk
Tell HTC
Tips for Home
T-Mobile Mall
Touch Input
Transfer
TTS Service
Twitter widget
Updater
Upgrade Setup
User Dictionary
https://market.android.c...
Device
App Usage
Application
Superuser
Related URL
https://market.android.com/details?id=com.noshufou.an
Storage
Device
Items: 152
Selected Items: 1
Ready
152 Running Apps
Superuser
(Evidence of rooting)


FLEXISPY
/data/system/usagedata/usage-20120207
contains a reference to: “com.android.msecurity”
Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
data
anr
backup
data
local
misc
property
system
appusagestats
dropbox
registered_services
shared_prefs
sync
throttle
usagestats
usage-19800106
usage-20120207
usage-20120217
usage-20120218
accounts.db
accounts.db-shm
accounts.db-wal
appwidgets.xml
batterystats.bin
called_pre_boots.dat
entropy.dat
packages.list
packages.xml
storage_reserve
uiderrors.txt
userbehavior.db
userbehavior.db-shm
userbehavior.xml
wallpaper_info.xml
devlog
Search [1 results]
Find:
Offset Length Value Sourc
1 0x31B 0x12 msecurity
Values Bookmarks Highlights Search Search [1 results]
Length: 0x180C Offset: 0x32E Selection: 0x2A


FLEXISPY
Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
Smart Phones_PDAs_Android - Method 1.zip
cache
data
anr
backup
data
local
misc
dm
calllog.ref
callmgrd.zip
config.dat
dev_id
event.db
fx.log
gmail.ref
license.db
logcat.log
maind.zip
pmond.zip
preference.db
s32
sms.ref
wifi
AccPrmsF.ini
AK8975Prms.ini
rild_nitz_long_name_310260
rild_nitz_short_name_310260
property
gmail.ref
fx.log
Hex View
File Info
Highlights
Find:
Offset Length Value
Values
Bookmarks
Highlights
/data/misc/dm/
callog.ref
callmgrd.zip
config.dat
dev_id
event.db
fx.log
gmail.ref
license.db
logcat.log
maind.zip
preference.db
s32
sms.ref

/data/misc/dm/fx.log



/data/misc/dm/fx.log

ATTRIBUTION!
Hidden SMS command & Registration Number

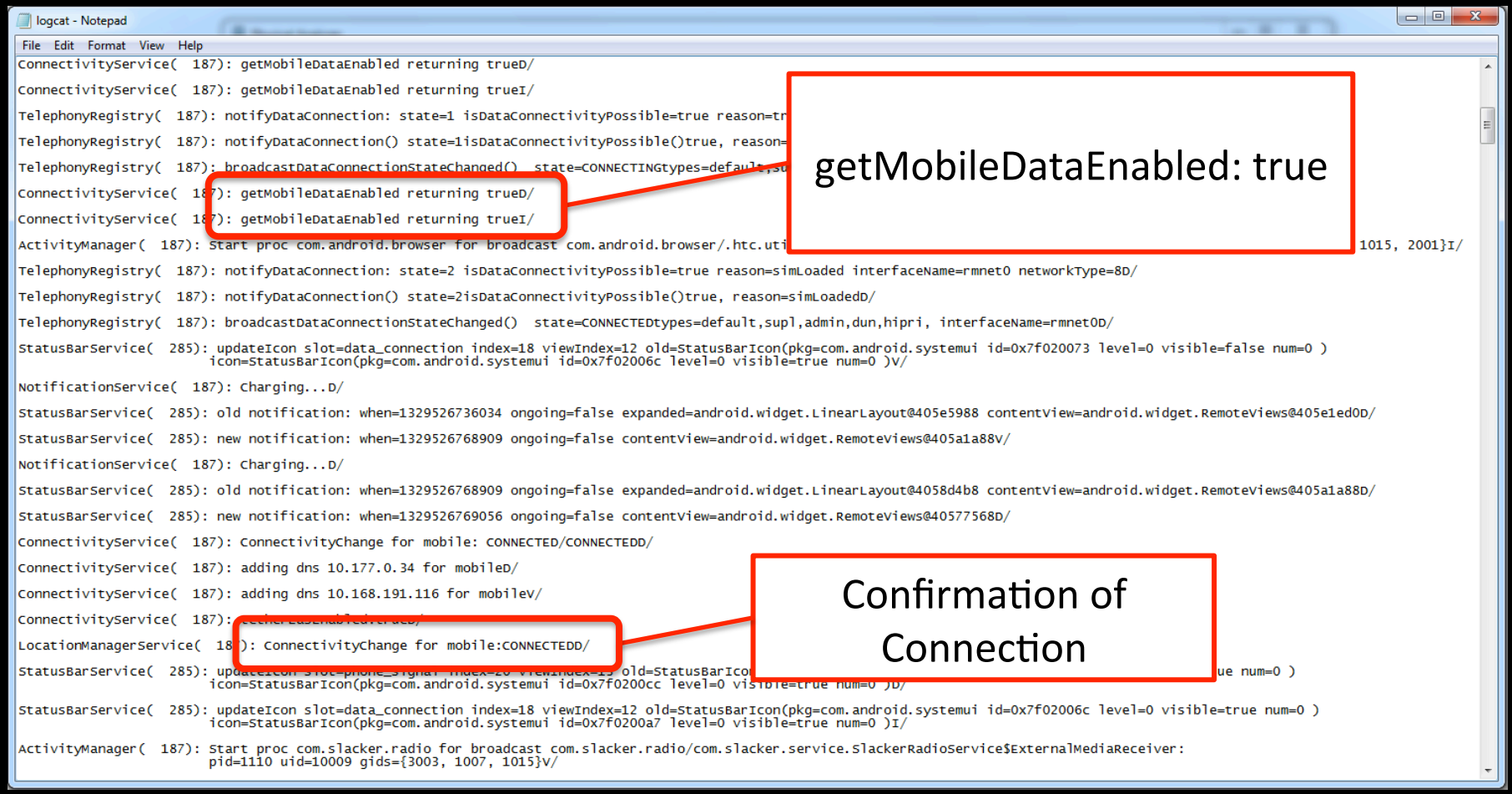
fx - Notepad

File Edit Format View Help

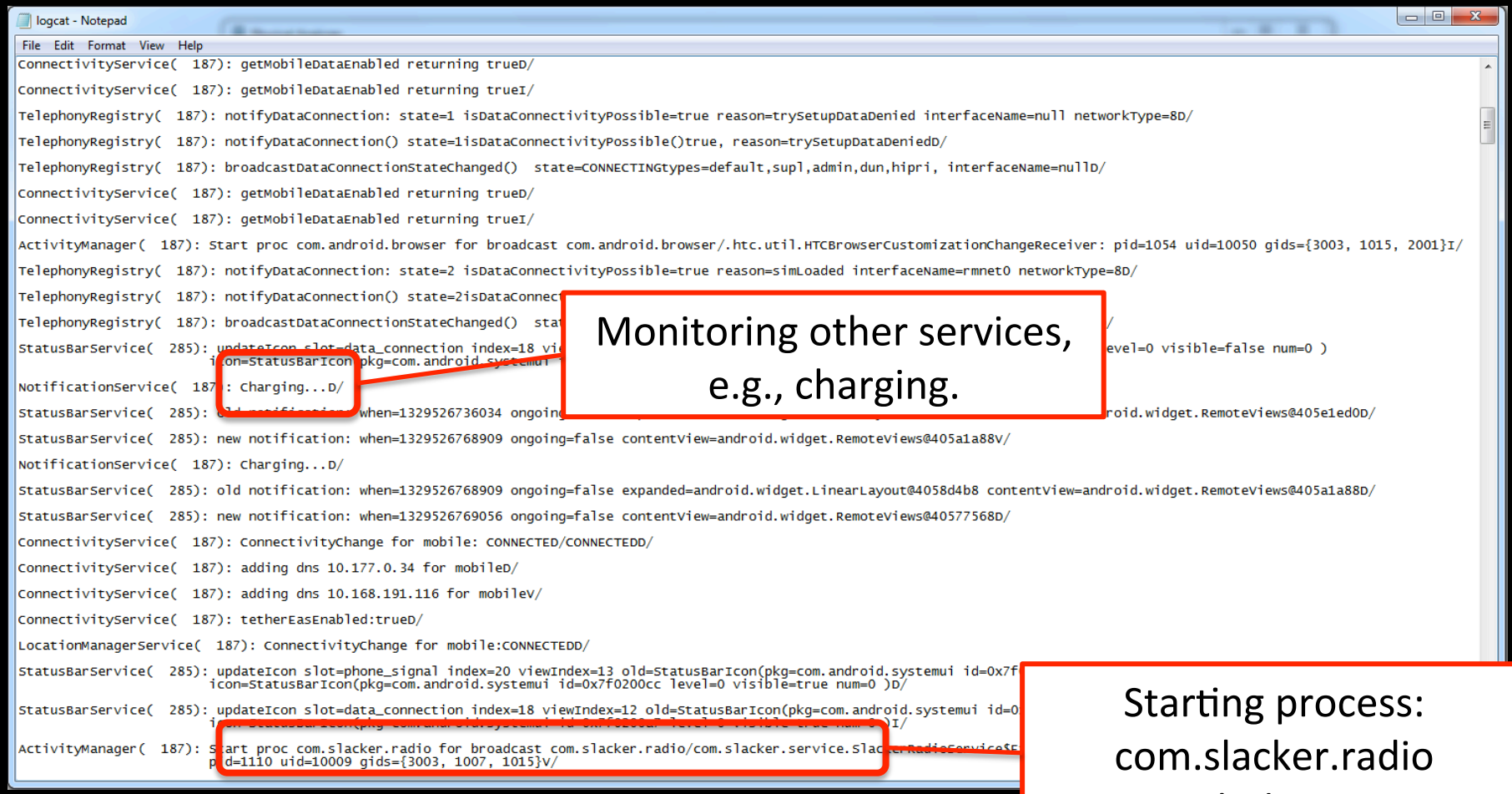
```
02-07 08:20:27.102: WARNING/SmsCommandHelper(2018): ==Current Settings==
02-07 08:20:27.102: WARNING/SmsCommandHelper(2018): Start Capture:Yes
02-07 08:20:27.102: WARNING/SmsCommandHelper(2018): Events:Call log,SMS,Ema
02-07 08:20:27.102: WARNING/SmsCommandHelper(2018): Timer:1hour
02-07 08:20:27.102: WARNING/SmsCommandHelper(2018): Max Event:10
02-07 08:20:27.308: WARNING/SmsObserver(2017): registerObserver # refId: 0
02-07 08:20:27.369: WARNING/ServiceManager(2017): enableCaptureEmail # ENTE
02-07 08:20:27.579: WARNING/ServiceManager(2017): enableCaptureIm # ENTER ...
02-07 08:20:27.709: WARNING/ServiceManager(2017): disableCaptureLocation # ENTER ...
02-07 08:20:27.730: WARNING/GpsTracking(2017): disable # ENTER ...
02-07 08:20:27.971: WARNING/EventDatabaseManager(2017): countTotalEvents # TYPE_CALL: 0, TYPE_SMS: 0, TYPE_EMAIL: 0,
                                                        TYPE_LOCATION: 0, TYPE_IM: 0, TYPE_SYSTEM: 2, Total: 2
02-07 08:20:27.979: WARNING/EventManager(2017): processNumberOfEvents # Number of events: 2 / 10
02-07 08:22:17.071: WARNING/SocketStmcSms(2067): Found a new SMS
02-07 08:22:17.090: WARNING/SocketStmcSms(2067): SMS Command is detected! -> Hide
02-07 08:22:17.109: WARNING/SmsCommandManager(2018): processSmsCommand # +15712[redacted]: <*#10><06107769[redacted]><+15712[redacted]><D>
02-07 08:22:17.104: WARNING/SocketStmcSms(2067): Forward SMS: false
02-07 08:22:17.805: WARNING/EventDatabaseManager(2017): countTotalEvents # TYPE_CALL: 0, TYPE_SMS: 0, TYPE_EMAIL: 0,
                                                        TYPE_LOCATION: 0, TYPE_IM: 0, TYPE_SYSTEM: 3, Total: 3
02-07 08:22:17.815: WARNING/EventManager(2017): processNumberOfEvents # Number of events: 3 / 10
02-07 08:22:21.020: WARNING/SocketStmcSms(2067): IsEnable: true, Edition: PROX
02-07 08:22:21.041: WARNING/SocketStmcCall(2067): IsEnable: true, Edition: PROX
02-07 08:22:21.126: WARNING/SocketStmcSms(2067): Set Monitor Number: "+15712[redacted]"
02-07 08:22:21.141: WARNING/SocketStmcCall(2067): Set Monitor Number: "+15712[redacted]"
02-07 08:22:21.196: WARNING/SmsCommandHelper(2018): sendResponse # response: [66 2.03.3][10] OK
02-07 08:22:21.196: WARNING/SmsCommandHelper(2018): ==Current Settings==
02-07 08:22:21.196: WARNING/SmsCommandHelper(2018): Call:Yes,+15712[redacted]
02-07 08:22:21.196: WARNING/SmsCommandHelper(2018): WL Status:Disabled
02-07 08:22:21.395: WARNING/SocketStmcSms(2067): Set keyword#1: ""
02-07 08:22:21.457: WARNING/SocketStmcSms(2067): Set keyword#2: ""
02-07 08:22:21.857: WARNING/EventDatabaseManager(2017): countTotalEvents # TYPE_CALL: 0, TYPE_SMS: 0, TYPE_EMAIL: 0,
                                                        TYPE_LOCATION: 0, TYPE_IM: 0, TYPE_SYSTEM: 4, Total: 4
02-07 08:22:21.865: WARNING/EventManager(2017): processNumberOfEvents # Number of events: 4 / 10
02-07 08:23:58.264: WARNING/SocketStmcSms(2067): Found a new SMS
02-07 08:23:58.283: WARNING/SocketStmcSms(2067): SMS Command is detected! -> Hide
02-07 08:23:58.299: WARNING/SocketStmcSms(2067): Forward SMS: false
02-07 08:23:58.308: WARNING/SmsCommandManager(2018): processSmsCommand # +15712[redacted]: <*#50><06107769[redacted]><1,0,0><D>
02-07 [redacted]ntTotalEvents # TYPE_CALL: 0, TYPE_SMS: 0, TYPE_EMAIL: 0,
02-07 [redacted]E_LOCATION: 0, TYPE_IM: 0, TYPE_SYSTEM: 5, Total: 5
02-07 [redacted]true, Edition: PROX
02-07 [redacted]erOfEvents # Number of events: 5 / 10
02-07 [redacted] true, Edition: PROX
02-07 [redacted]true, Edition: PROX
02-07 [redacted] true, Edition: PROX
02-07 [redacted]r Number "+15712[redacted]"
02-07 [redacted]or Numbe: "+15712[redacted]"
02-07 [redacted]r Number "+15712[redacted]"
02-07 [redacted]or Numbe "+1571[redacted]"
02-07 [redacted]true, Edition: PROX
02-07 [redacted] true, Edition: PROX
02-07 08:24:00.240: WARNING/SocketStmcSms(2067): Set keyword#1: ""
02-07 08:24:00.334: WARNING/SocketStmcSms(2067): Set keyword#1: ""
02-07 08:24:00.429: WARNING/SocketStmcSms(2067): Set Monitor Number: "+15712[redacted]"
02-07 08:24:00.465: WARNING/SocketStmcCall(2067): Set Monitor Number: "+1571[redacted]"
02-07 08:24:00.488: WARNING/SocketStmcSms(2067): Set keyword#2: ""
```

ATTRIBUTION!
Monitoring number

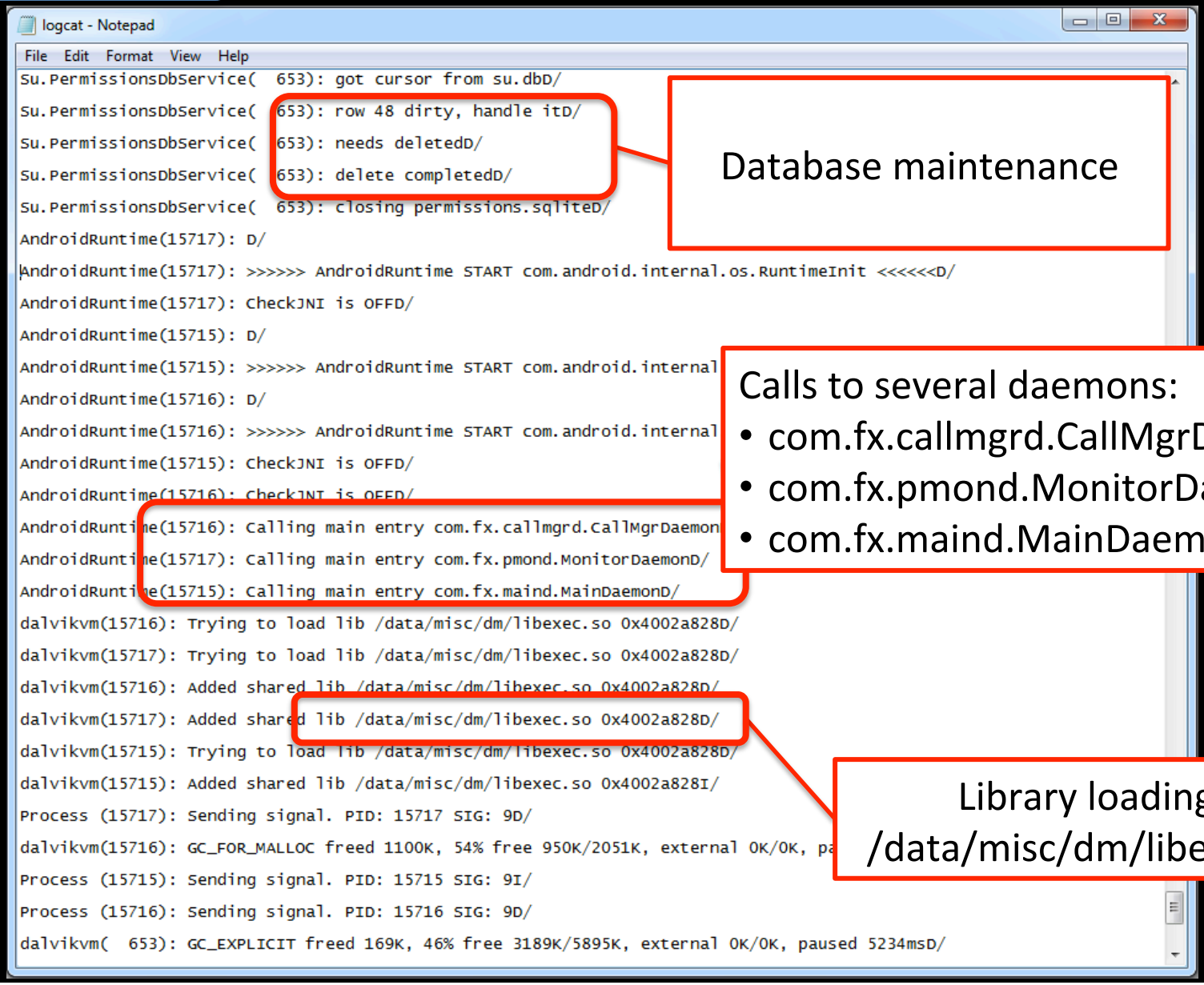
/data/misc/dm/logcat



/data/misc/dm/logcat



/data/misc/dm/logcat



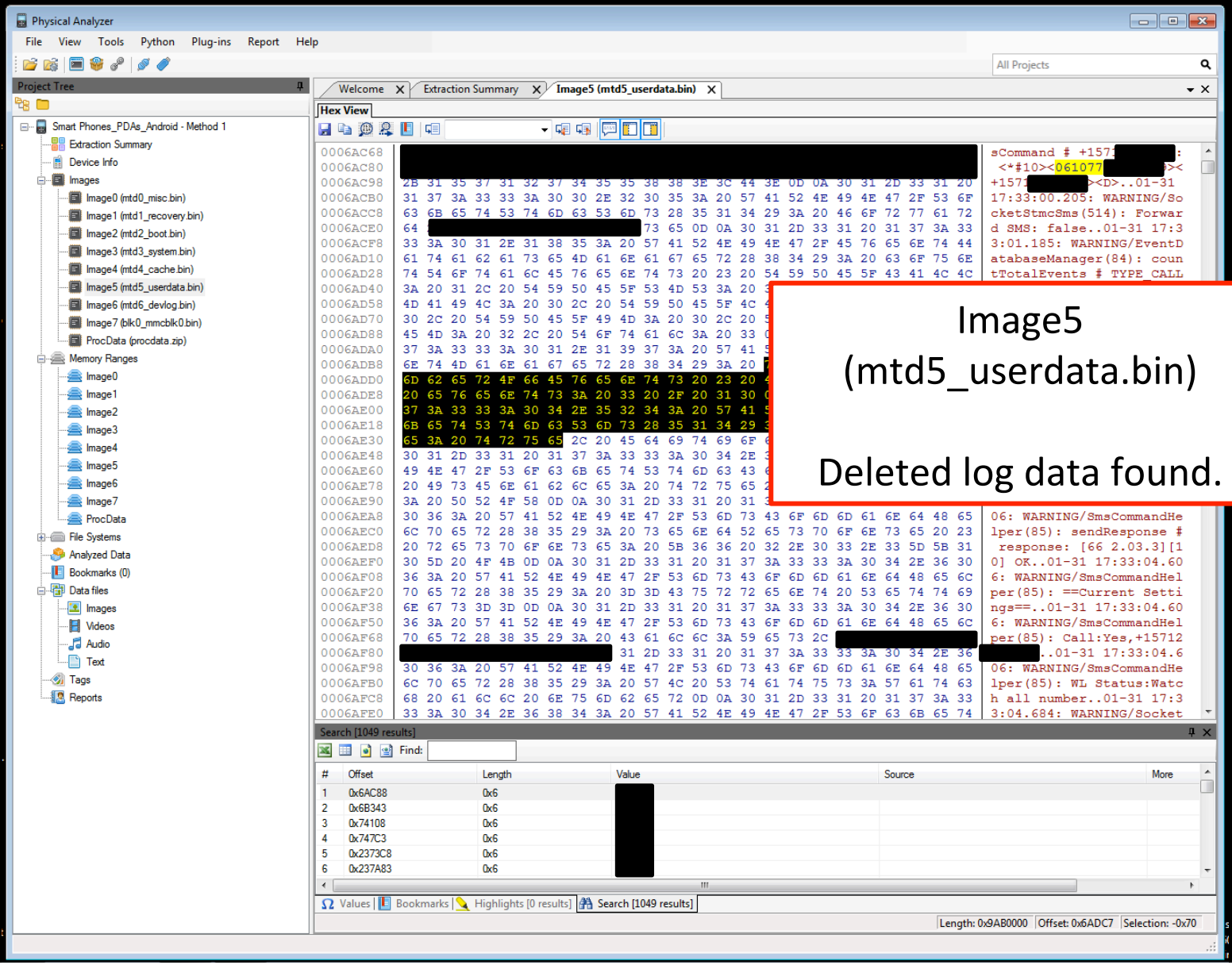


Image5
(mtd5_userdata.bin)

Deleted log data found.


01-31 17:59:11.043: WARNING/SimChangeThread(514): verifySim # Previous subscriber ID: 3102[redacted]..
01-31 17:59:12.426: WARNING/SimChangeThread(514): verifySim # Current subscriber ID: 3102[redacted]..
01-31 17:59:12.897: WARNING/SimChangeThread(514): verifySim # SIM is not changed..
01-31 18:18:20.805: WARNING/SocketStmcSms(514): Found a new SMS..
01-31 18:18:20.837: WARNING/SocketStmcSms(514): SMS Command is detected! -> Hide..
01-31 18:18:20.890: WARNING/SocketStmcSms(514): Forward SMS: false..
01-31 18:18:20.909: WARNING/SmsCommandManager(85): processSmsCommand # +1571[redacted] <*#67><061077[redacted]><D>..
01-31 18:18:22.783: WARNING/EventDatabaseManager(84): countTotalEvents # TYPE_CALL: 2, TYPE_SMS: 0, TYPE_EMAIL: 0, TYPE_LOCATION: 0, TYPE_IM: 0, TYPE_SYSTEM: 8, Total: 10..
01-31 18:18:22.809: WARNING/EventManager(84): processNumberOfEvents # Number of events: 10 / 10..
01-31 18:18:22.880: WARNING/EventManager(84): processNumberOfEvents # Request deliver all events..
01-31 18:18:23.294: WARNING/EventDatabaseManager(84): countTotalEvents # TYPE_CALL: 2, TYPE_SMS: 0, TYPE_EMAIL: 0, TYPE_LOCATION: 0, TYPE_IM: 0, TYPE_SYSTEM: 8, Total: 10
****
of events: 4 / 10..
01-31 12:29:11.059: WARNING/SocketStmcSms(584): IsEnable: true, Edition: PROX..
01-31 12:29:11.093: WARNING/SocketStmcSms(584): Set keyword#1: ""..
01-31 12:29:11.122: WARNING/SocketStmcCall(584): IsEnable: true, Edition: PROX..
01-31 12:29:11.162: WARNING/SocketStmcSms(584): Set keyword#1: ""..
01-31 12:29:11.205: WARNING/SocketStmcSms(584): Set keyword#2: ""..
01-31 12:29:11.292: WARNING/SocketStmcSms(584): Set keyword#2: ""..
01-31 12:29:11.323: WARNING/SocketStmcSms(584): Set Monitor Number: "+1571[redacted]"..
01-31 12:29:11.364: WARNING/SmsCommandHelper(85): sendResponse # response: [66 2.03.3][50] OK..
01-31 12:29:11.364: WARNING/SmsCommandHelper(85): ==Current Settings==..
01-31 12:29:11.364: WARNING/SmsCommandHelper(85): WL Status:Watch all numbe...
01-31 12:29:11.349: WARNING/SocketStmcCall(584): Set Monitor Number: "+1571[redacted]"..
01-31 12:29:11.659: WARNING/SocketStmcSms(584): Set keyword#1: ""..
01-31 12:29:11.716: WARNING/SocketStmcSms(584): Set keyword#2: ""..
SIM Card check
Spyware version
Instructions

01-31 17:59:11.043: WARNING/SimChangeThread(514): verifySim # Previous subscriber ID: 3102[redacted]..

01-31 17:59:12.426: WARNING/SimChangeThread(514): verifySim # Current subscriber ID: 3102[redacted]..

01-31 17:59:12.897: WARNING/SimChangeThread(514): verifySim # SIM is not changed..

01-31 18:18:20.805: WARNING/SocketStmcSms(514): Found a new SMS..

01-31 18:18:20.837: WARNING/SocketStmcSms(514): SMS Command is detected! -> Hide..

01-31 18:18:20.890: WARNING/SocketStmcSms(514): Forward SMS: false..

01-31 18:18:20.909: WARNING/SmsCommandManager(85): processSmsCommand # +1571[redacted] <*#67><

01-31 18:18:22.783: WARNING/EventDatabaseManager(84): countTotalEvents # TYPE_CALL: 2, TYPE_SMS: 0, TYPE_EMAIL: 0, TYPE_LOCATION:

ATTRIBUTION!
Controlling Number

berOfEvents # Number of events: 10 / 10..

berOfEvents # Request deliver all events..

ntTotalEvents # TYPE_CALL: 2, TYPE_SMS: 0, TYPE_EMAIL: 0, TYPE_LOCATION:

****

of events: 4 / 10..

01-31 12:29:11.059: WARNING/SocketStmcSms(584): IsEnable: true, Edition: PROX..

01-31 12:29:11.093: WARNING/SocketStmcSms(584): Set keyword#1: ""..

01-31 12:29:11.122: WARNING/SocketStmcCall(584): IsEnable: true, Edition: PROX..

01-31 12:29:11.162: WARNING/SocketStmcSms(584): Set keyword#1: ""..

01-31 12:29:11.205: WARNING/SocketStmcSms(584): Set keyword#2: ""..

01-31 12:29:11.292: WARNING/SocketStmcSms(584): Set keyword#2: ""..

01-31 12:29:11.323: WARNING/SocketStmcSms(584): Set Monitor Number: "+1571[redacted]"..

01-31 12:29:11.364: WARNING/SmsCommandHelper(85): sendResponse # response: [66 2.03.3][50] OK..

01-31 12:29:11.364: WARNING/SmsCommandHelper(85): ==Current Settings==..

01-31 12:29:11.364: WARNING/SmsCommandHelper(85): WL Status:Watch all number..

01-31 12:29:11.349: WARNING/SocketStmcCall(584): Set Monitor Number: "+1571[redacted]"..

01-31 12:29:11.659: WARNING/SocketStmcSms(584): Set keyword#1: ""..

01-31 12:29:11.716: WARNING/SocketStmcSms(584): Set keyword#2: ""..

SMS Commands

Auto-reply


SpyBubble
La Verdad Al Descubierto

URL history

http://www.spybubble.com/android/adv/radio.apk

downloads.db entry

uri: http://www.spybubble.com/android/adv/radio.apk

hint: radio.apk

_data: /mnt/sdcard/Download/radio.apk

(Phone not shipped with an SD Card.)

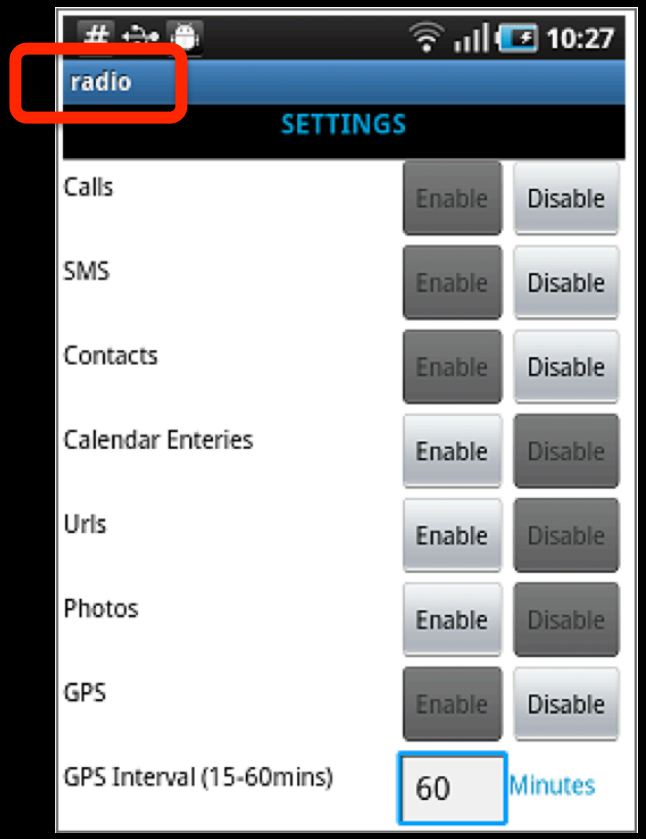
A couple of glitches…

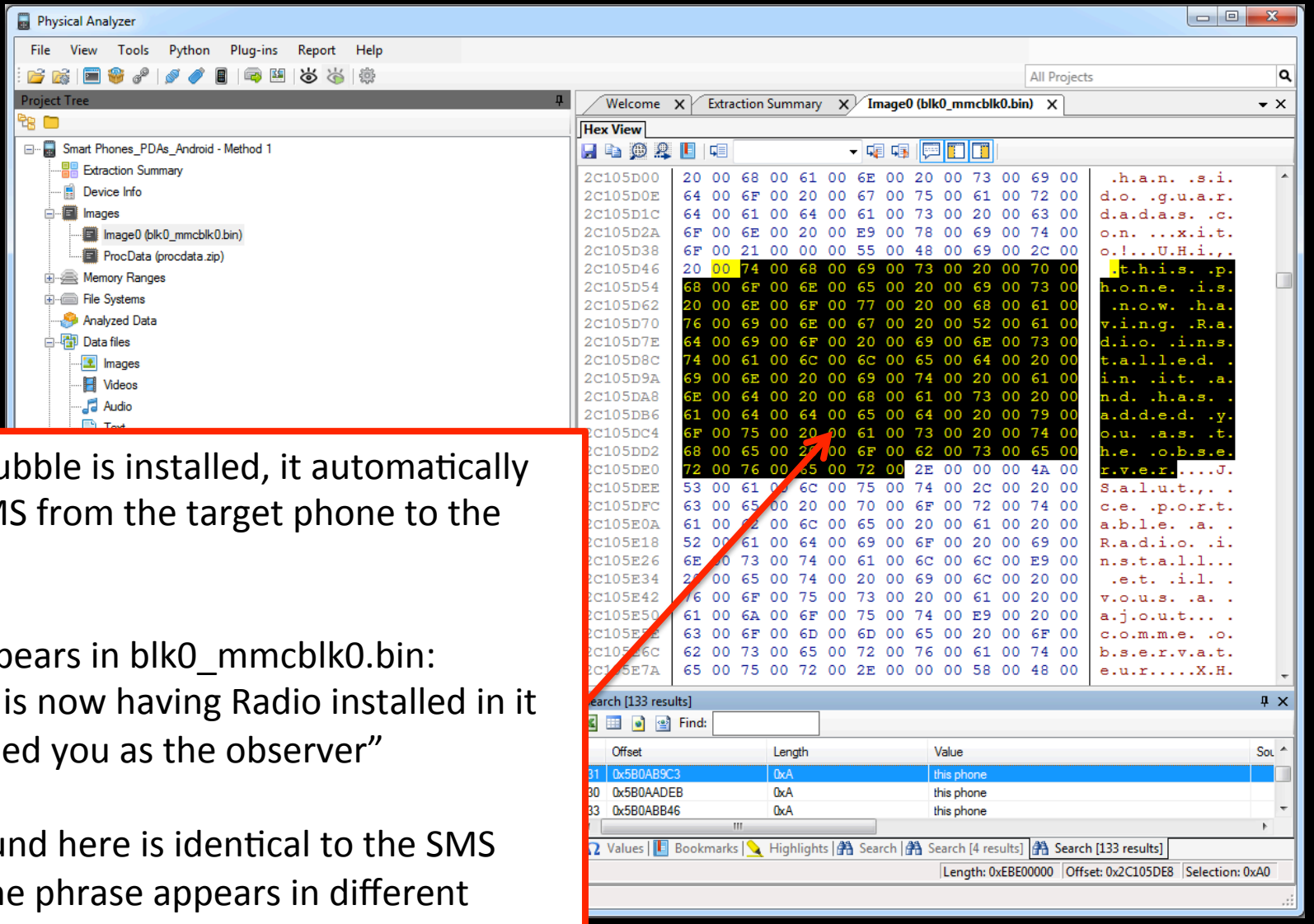
Outgoing call log #999999*

There was an error with the operation of the software.

This should not appear in the log.

This number can be changed.
Regardless of the number, it will start with # and end with *.

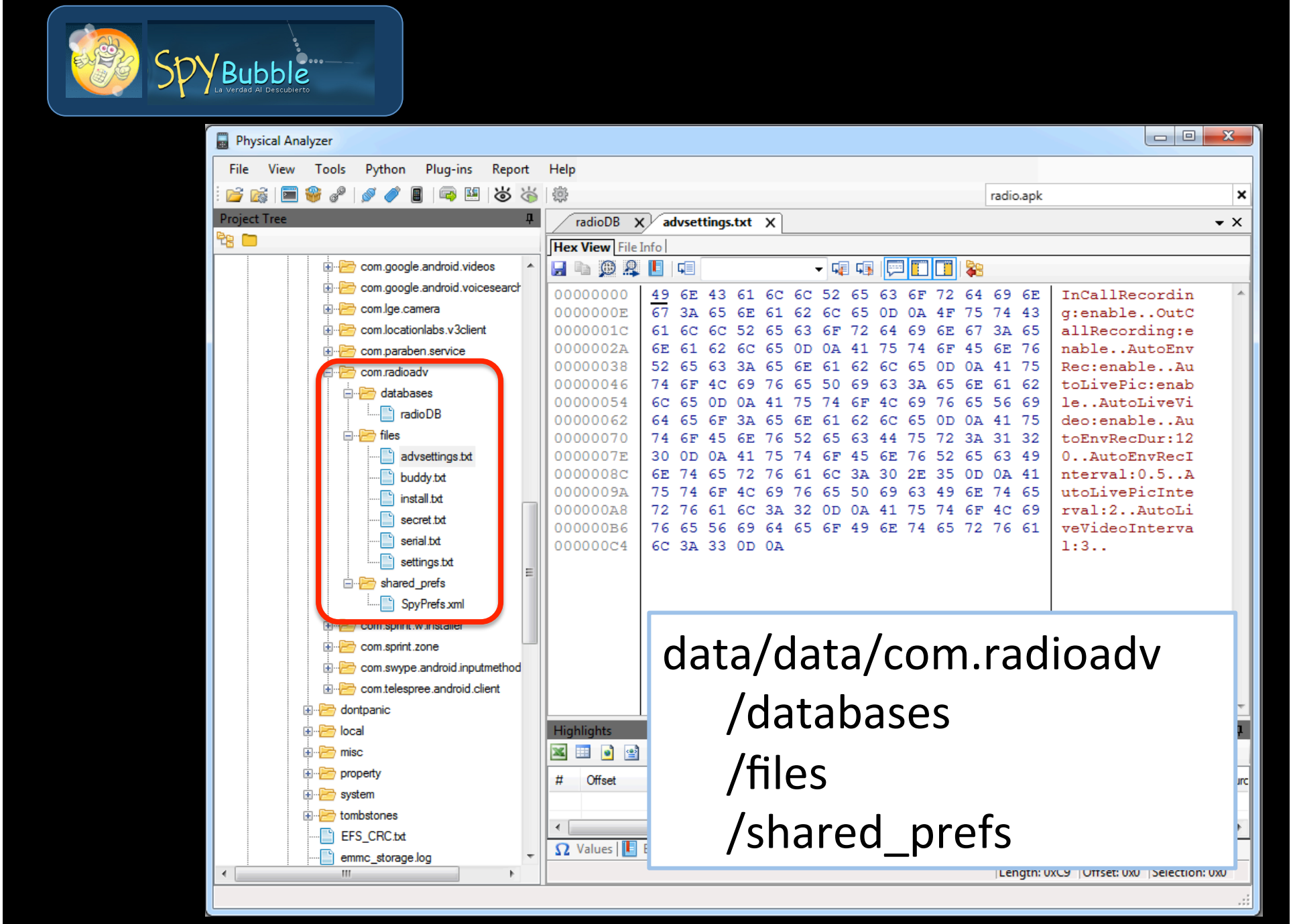


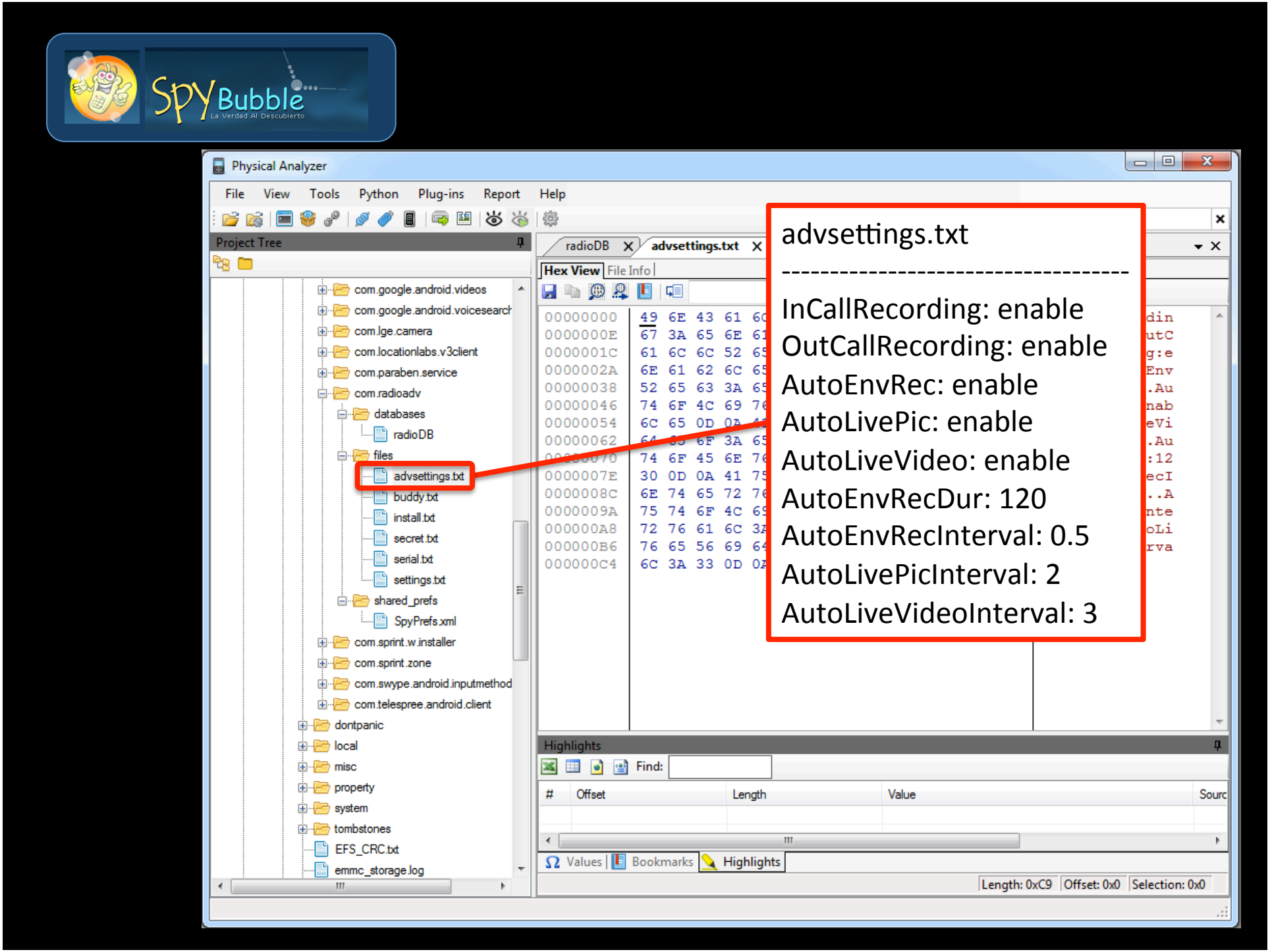


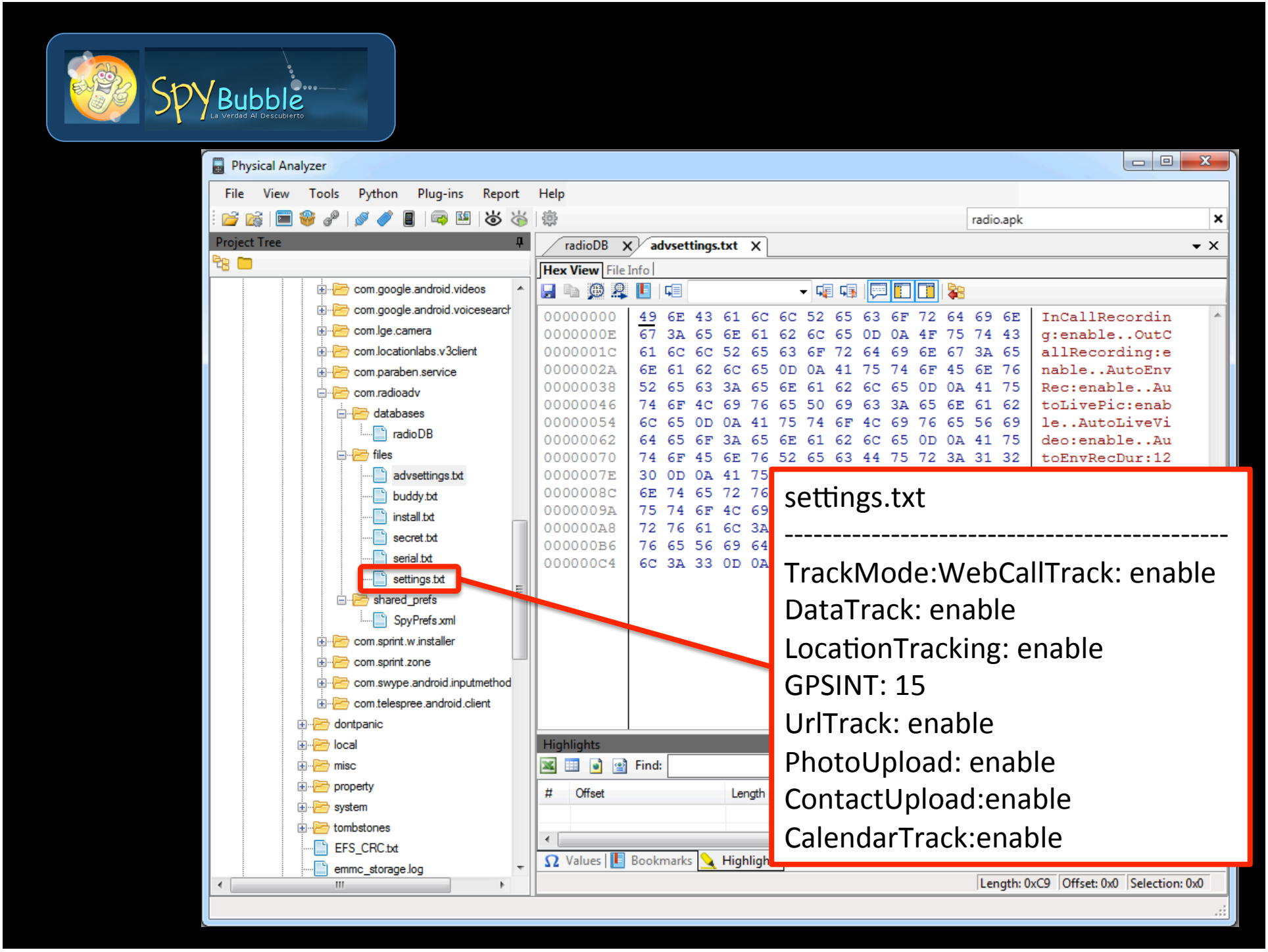
When SpyBubble is installed, it automatically sends an SMS from the target phone to the observer.

This text appears in blk0_mmcblk0.bin: “this phone is now having Radio installed in it and has added you as the observer”

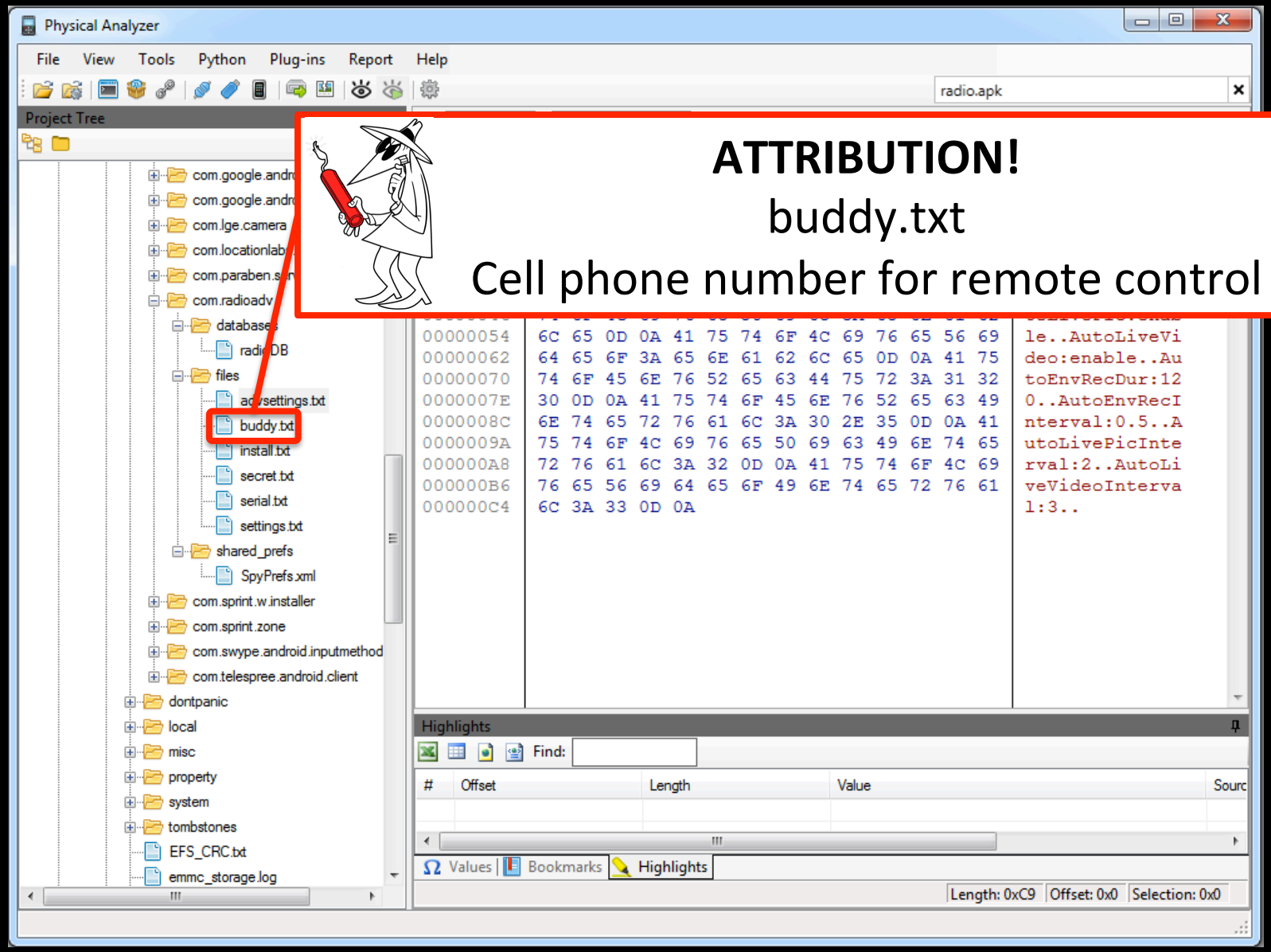
This text found here is identical to the SMS message. The phrase appears in different languages before and after the English version.


SpyBubble
La Verdad Al Descubierto
Physical Analyzer
File View Tools Python Plug-ins Report Help
radio.apk
Project Tree
com.google.android.videos
com.google.android.voicesearch
com.lge.camera
com.locationlabs.v3client
com.paraben.service
com.radioadv
databases
radioDB
files
advsettings.txt
buddy.txt
install.txt
secret.txt
serial.txt
settings.txt
shared_prefs
SpyPrefs.xml
com.sprint.zone
com.swype.android.inputmethod
com.telespree.android.client
dontpanic
local
misc
property
system
tombstones
EFS_CRC.txt
emmc_storage.log
radioDB
advsettings.txt
Hex View
File Info
00000000 49 6E 43 61 6C 6C 52 65 63 6F 72 64 69 6E InCallRecordin
0000000E 67 3A 65 6E 61 62 6C 65 0D 0A 4F 75 74 43 g:enable..OutC
0000001C 61 6C 6C 52 65 63 6F 72 64 69 6E 67 3A 65 allRecording:e
0000002A 6E 61 62 6C 65 0D 0A 41 75 74 6F 45 6E 76 nable..AutoEnv
00000038 52 65 63 3A 65 6E 61 62 6C 65 0D 0A 41 75 Rec:enable..Au
00000046 74 6F 4C 69 76 65 50 69 63 3A 65 6E 61 62 toLivePic:enab
00000054 6C 65 0D 0A 41 75 74 6F 4C 69 76 65 56 69 le..AutoLiveVi
00000062 64 65 6F 3A 65 6E 61 62 6C 65 0D 0A 41 75 deo:enable..Au
00000070 74 6F 45 6E 76 52 65 63 44 75 72 3A 31 32 toEnvRecDur:12
0000007E 30 0D 0A 41 75 74 6F 45 6E 76 52 65 63 49 0..AutoEnvRecI
0000008C 6E 74 65 72 76 61 6C 3A 30 2E 35 0D 0A 41 nterval:0.5..A
0000009A 75 74 6F 4C 69 76 65 50 69 63 49 6E 74 65 utoLivePicInte
000000A8 72 76 61 6C 3A 32 0D 0A 41 75 74 6F 4C 69 rval:2..AutoLi
000000B6 76 65 56 69 64 65 6F 49 6E 74 65 72 76 61 veVideoInterva
000000C4 6C 3A 33 0D 0A l:3..
Highlights
Offset
Values
data/data/com.radioadv
/databases
/files
/shared_prefs


SpyBubble
La Verdad Al Descubierto
Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
com.google.android.videos
com.google.android.voicesearch
com.lge.camera
com.locationlabs.v3client
com.paraben.service
com.radioadv
databases
radioDB
files
advsettings.txt
buddy.txt
install.txt
secret.txt
serial.txt
settings.txt
shared_prefs
SpyPrefs.xml
com.sprint.w.installer
com.sprint.zone
com.swype.android.inputmethod
com.telespree.android.client
dontpanic
local
misc
property
system
tombstones
EFS_CRC.txt
emmc_storage.log
radioDB
advsettings.txt
Hex View
File Info
00000000 49 6E 43 61 6C
0000000E 67 3A 65 6E 61
0000001C 61 6C 6C 52 65
0000002A 6E 61 62 6C 65
00000038 52 65 63 3A 65
00000046 74 6F 4C 69 76
00000054 6C 65 0D 0A
00000062
00000070 74 6F 45 6E 76
0000007E 30 0D 0A 41 75
0000008C 6E 74 65 72 76
0000009A 75 74 6F 4C 69
000000A8 72 76 61 6C 3A
000000B6 76 65 56 69 64
000000C4 6C 3A 33 0D 0A
Highlights
Find:
Offset Length Value
Values Bookmarks Highlights
Length: 0xC9 Offset: 0x0 Selection: 0x0
advsettings.txt
InCallRecording: enable
OutCallRecording: enable
AutoEnvRec: enable
AutoLivePic: enable
AutoLiveVideo: enable
AutoEnvRecDur: 120
AutoEnvRecInterval: 0.5
AutoLivePicInterval: 2
AutoLiveVideoInterval: 3


SpyBubble
La Verdad Al Descubierto
Physical Analyzer
File View Tools Python Plug-ins Report Help
radio.apk
Project Tree
radioDB
advsettings.txt
Hex View
File Info
com.google.android.videos
com.google.android.voicesearch
com.lge.camera
com.locationlabs.v3client
com.paraben.service
com.radioadv
databases
radioDB
files
advsettings.txt
buddy.txt
install.txt
secret.txt
serial.txt
settings.txt
shared_prefs
SpyPrefs.xml
com.sprint.w.installer
com.sprint.zone
com.swype.android.inputmethod
com.telespree.android.client
dontpanic
local
misc
property
system
tombstones
EFS_CRC.txt
emmc_storage.log
00000000 49 6E 43 61 6C 6C 52 65 63 6F 72 64 69 6E InCallRecordin
0000000E 67 3A 65 6E 61 62 6C 65 0D 0A 4F 75 74 43 g:enable..OutC
0000001C 61 6C 6C 52 65 63 6F 72 64 69 6E 67 3A 65 allRecording:e
0000002A 6E 61 62 6C 65 0D 0A 41 75 74 6F 45 6E 76 nable..AutoEnv
00000038 52 65 63 3A 65 6E 61 62 6C 65 0D 0A 41 75 Rec:enable..Au
00000046 74 6F 4C 69 76 65 50 69 63 3A 65 6E 61 62 toLivePic:enab
00000054 6C 65 0D 0A 41 75 74 6F 4C 69 76 65 56 69 le..AutoLiveVi
00000062 64 65 6F 3A 65 6E 61 62 6C 65 0D 0A 41 75 deo:enable..Au
00000070 74 6F 45 6E 76 52 65 63 44 75 72 3A 31 32 toEnvRecDur:12
0000007E 30 0D 0A 41 75
0000008C 6E 74 65 72 76
0000009A 75 74 6F 4C 69
000000A8 72 76 61 6C 3A
000000B6 76 65 56 69 64
000000C4 6C 3A 33 0D 0A
Highlights
Find:
Offset Length
Values Bookmarks Highligh
Length: 0xC9 Offset: 0x0 Selection: 0x0
settings.txt
TrackMode:WebCallTrack: enable
DataTrack: enable
LocationTracking: enable
GPSINT: 15
UrlTrack: enable
PhotoUpload: enable
ContactUpload:enable
CalendarTrack:enable

/data/data/com.radioadv/files/

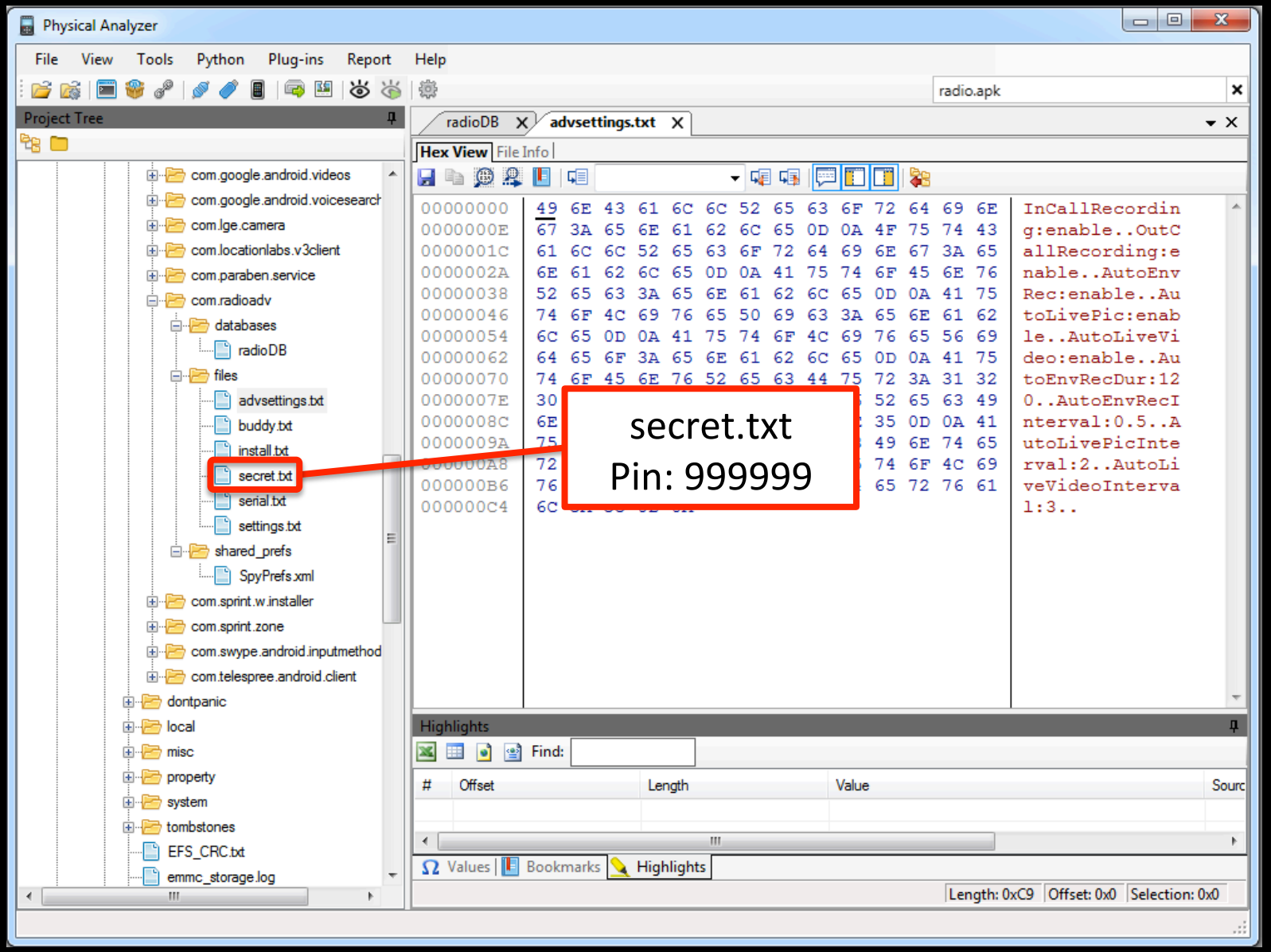


ATTRIBUTION!

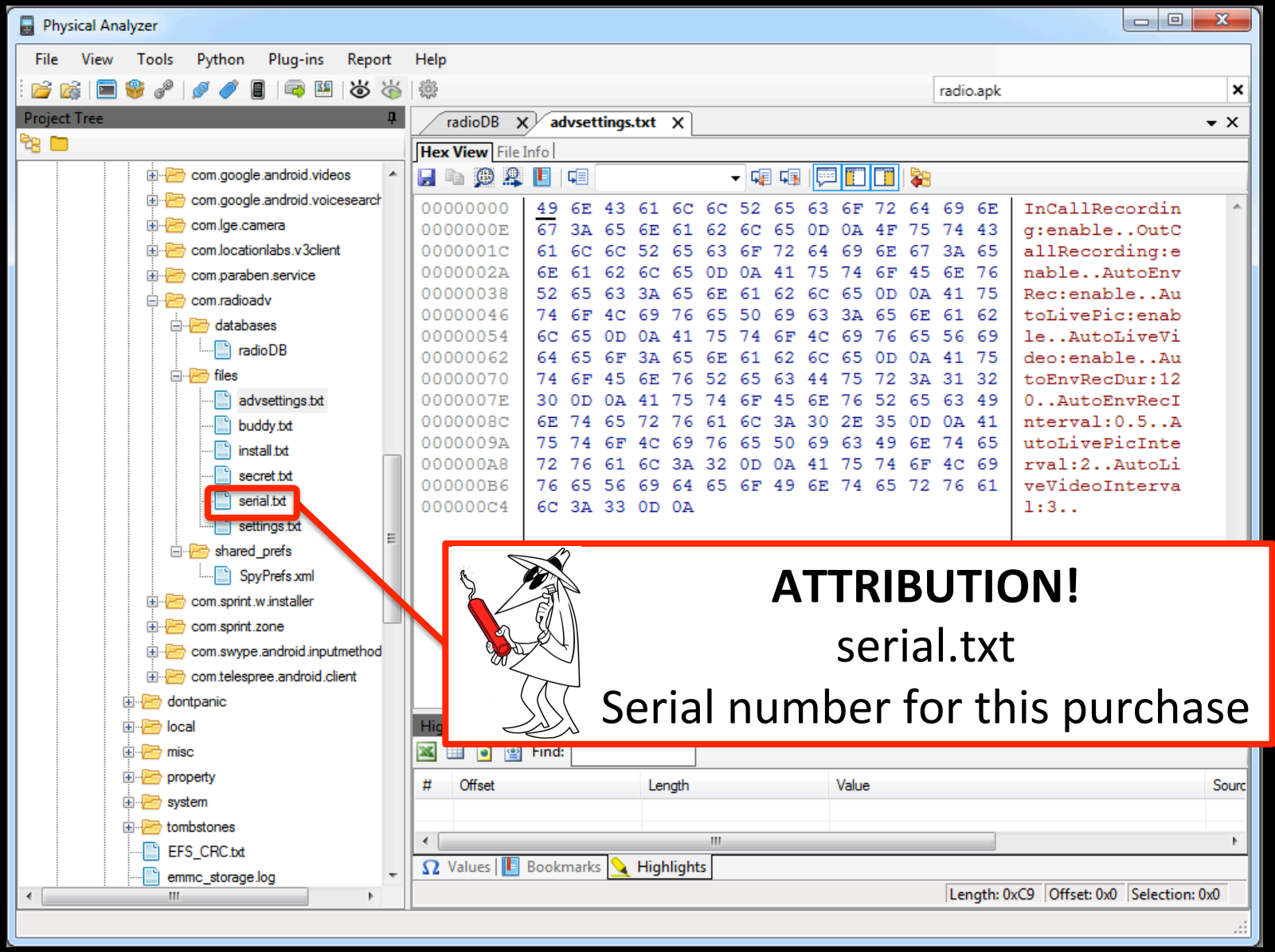
buddy.txt

Cell phone number for remote control

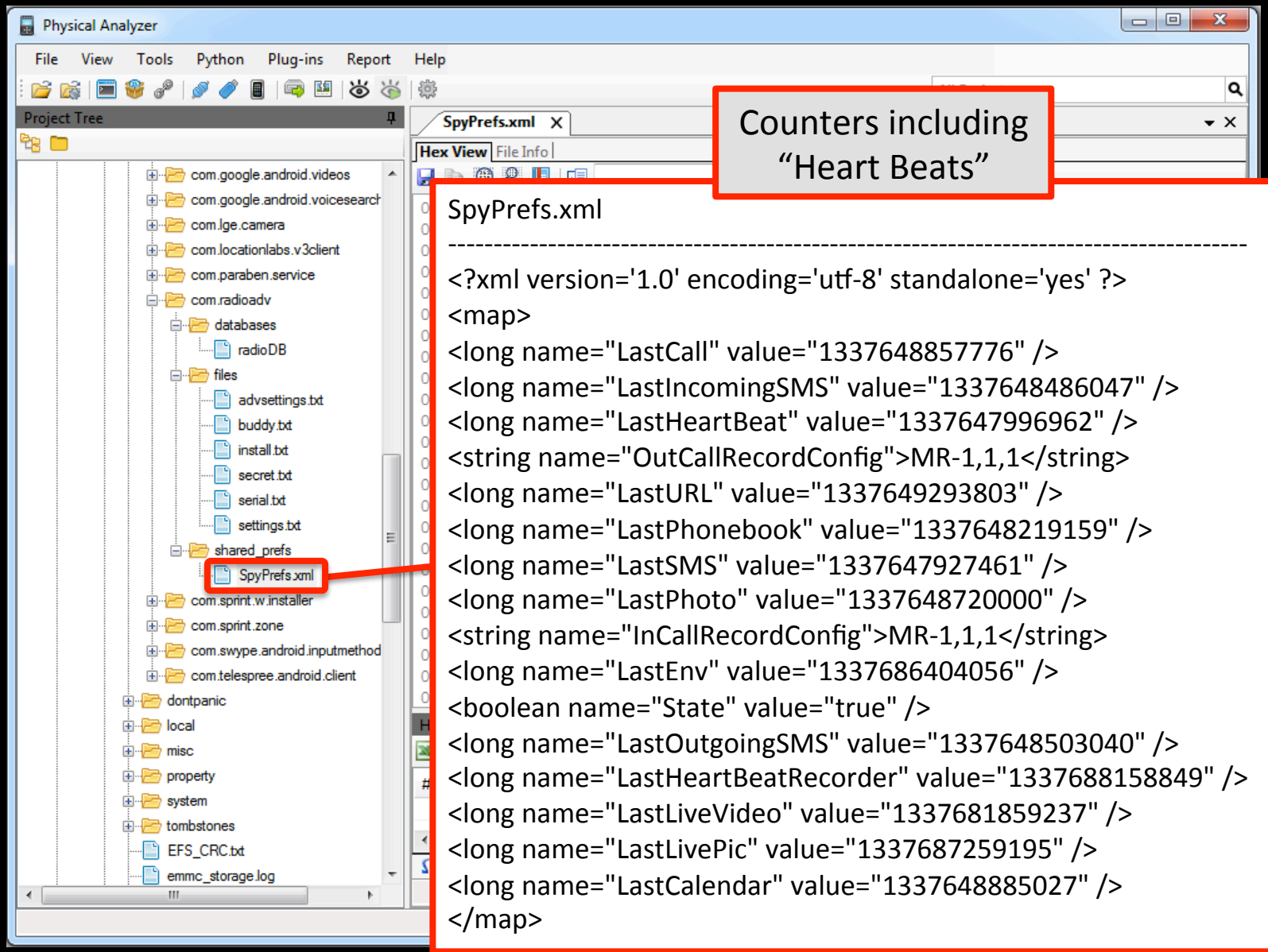
/data/data/com.radioadv/files/



/data/data/com.radioadv/files/



/data/data/com.radioadv/shared_prefs/



Counters including "Heart Beats"

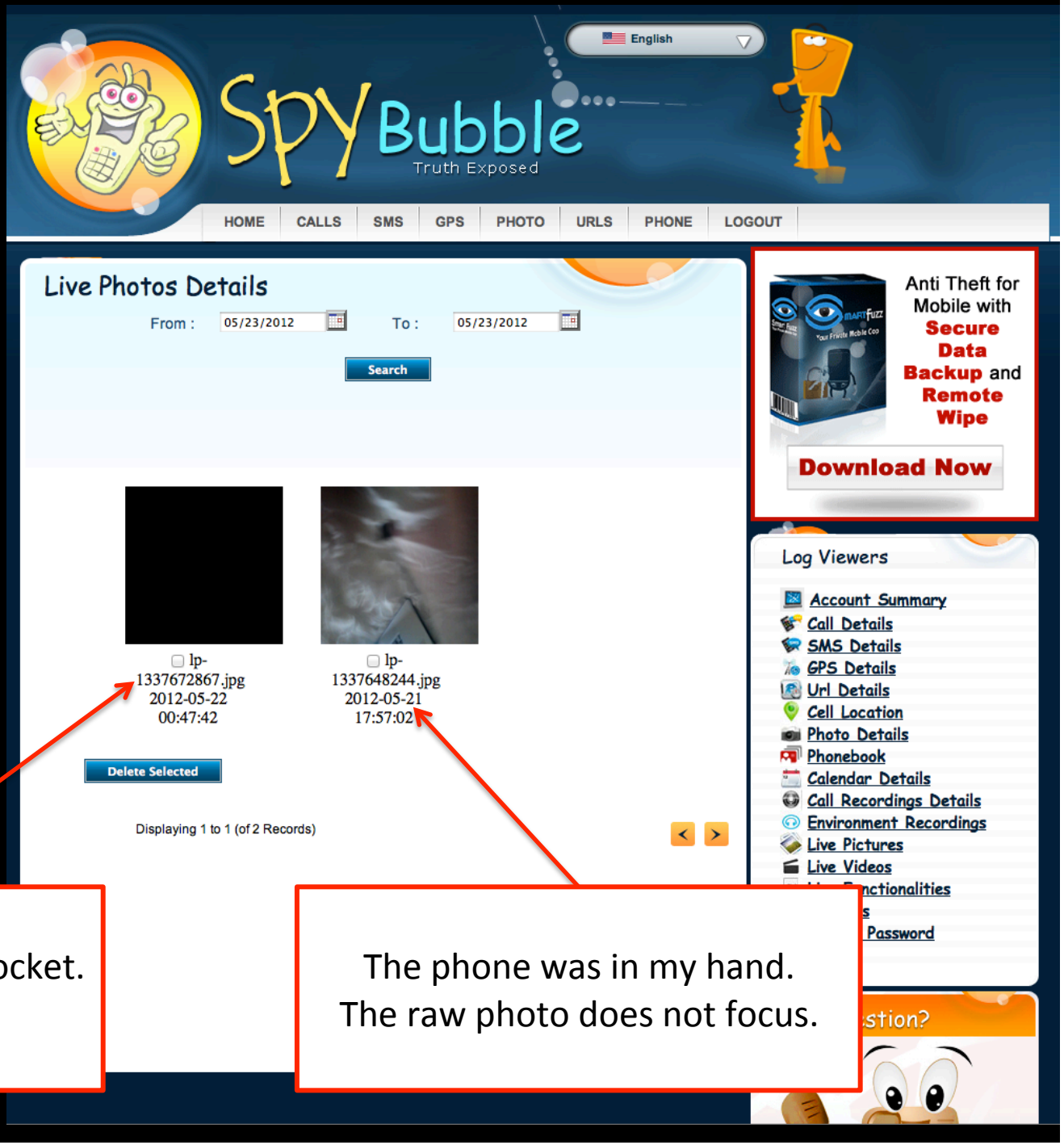
SpyPrefs.xml

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<long name="LastCall" value="1337648857776" />
<long name="LastIncomingSMS" value="1337648486047" />
<long name="LastHeartBeat" value="1337647996962" />
<string name="OutCallRecordConfig">MR-1,1,1</string>
<long name="LastURL" value="1337649293803" />
<long name="LastPhonebook" value="1337648219159" />
<long name="LastSMS" value="1337647927461" />
<long name="LastPhoto" value="1337648720000" />
<string name="InCallRecordConfig">MR-1,1,1</string>
<long name="LastEnv" value="1337686404056" />
<boolean name="State" value="true" />
<long name="LastOutgoingSMS" value="1337648503040" />
<long name="LastHeartBeatRecorder" value="1337688158849" />
<long name="LastLiveVideo" value="1337681859237" />
<long name="LastLivePic" value="1337687259195" />
<long name="LastCalendar" value="1337648885027" />
</map>
```

Live capture pictures:

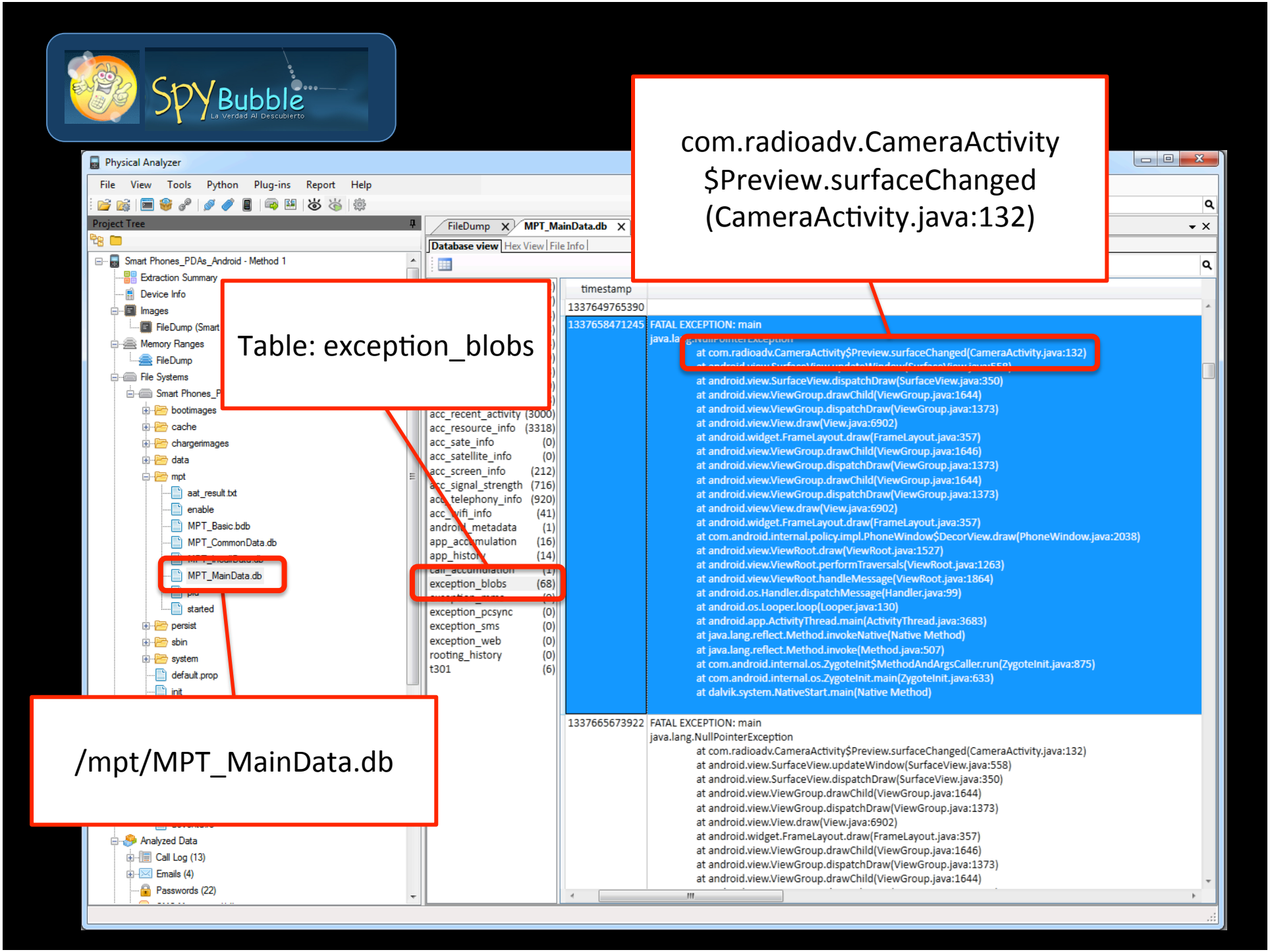
Retrieved from the website.

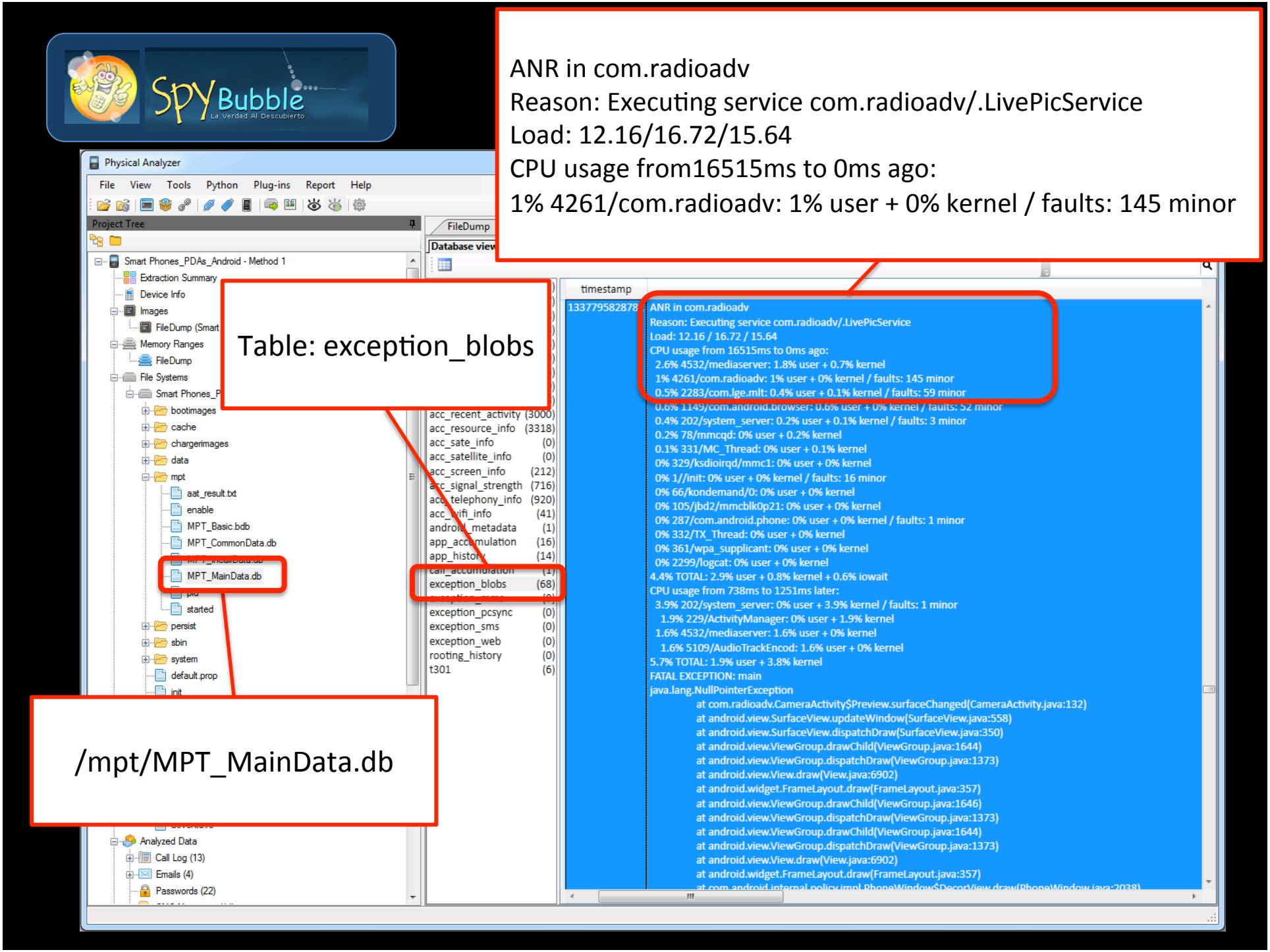
Not recovered from the phone.

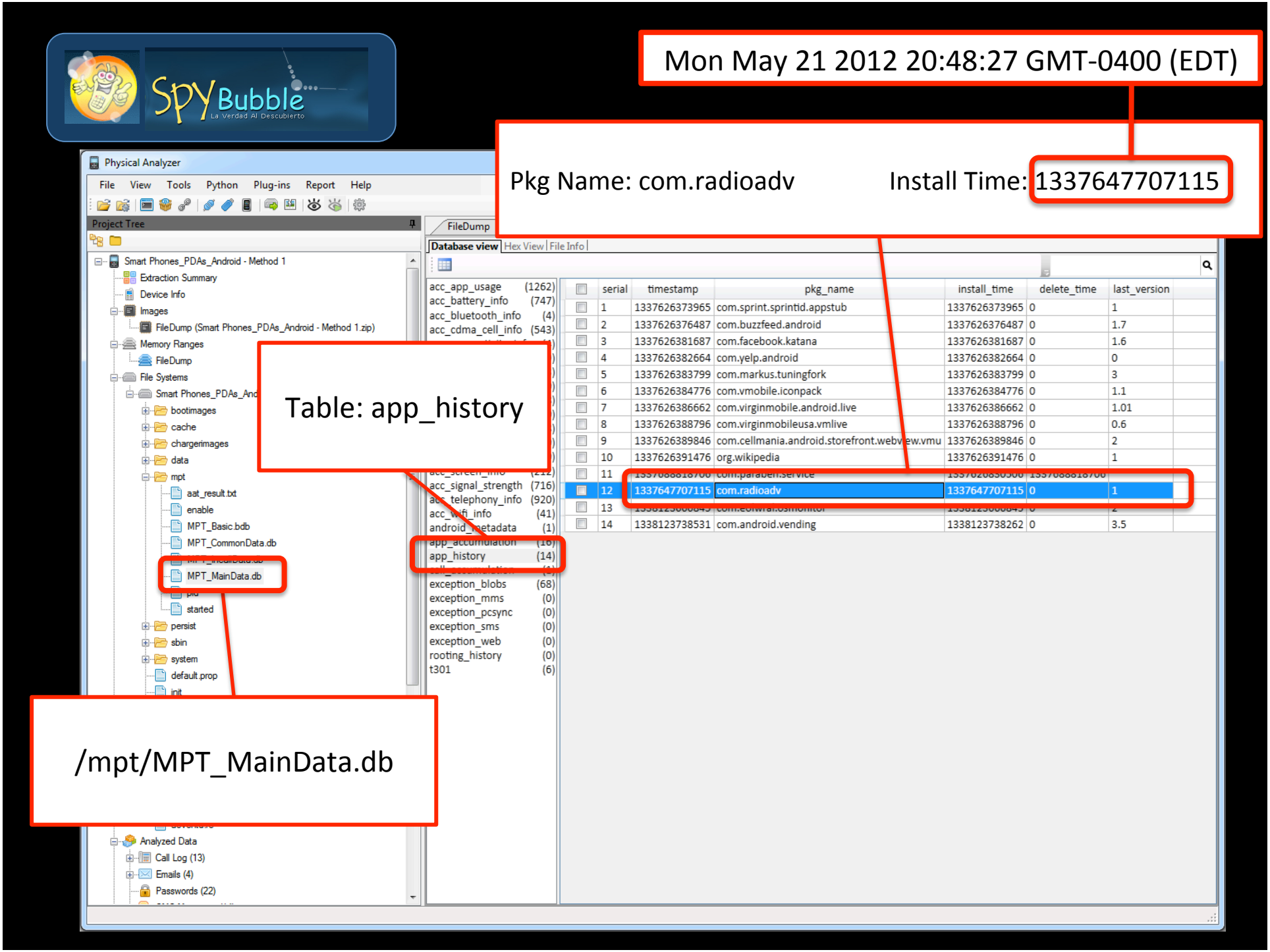


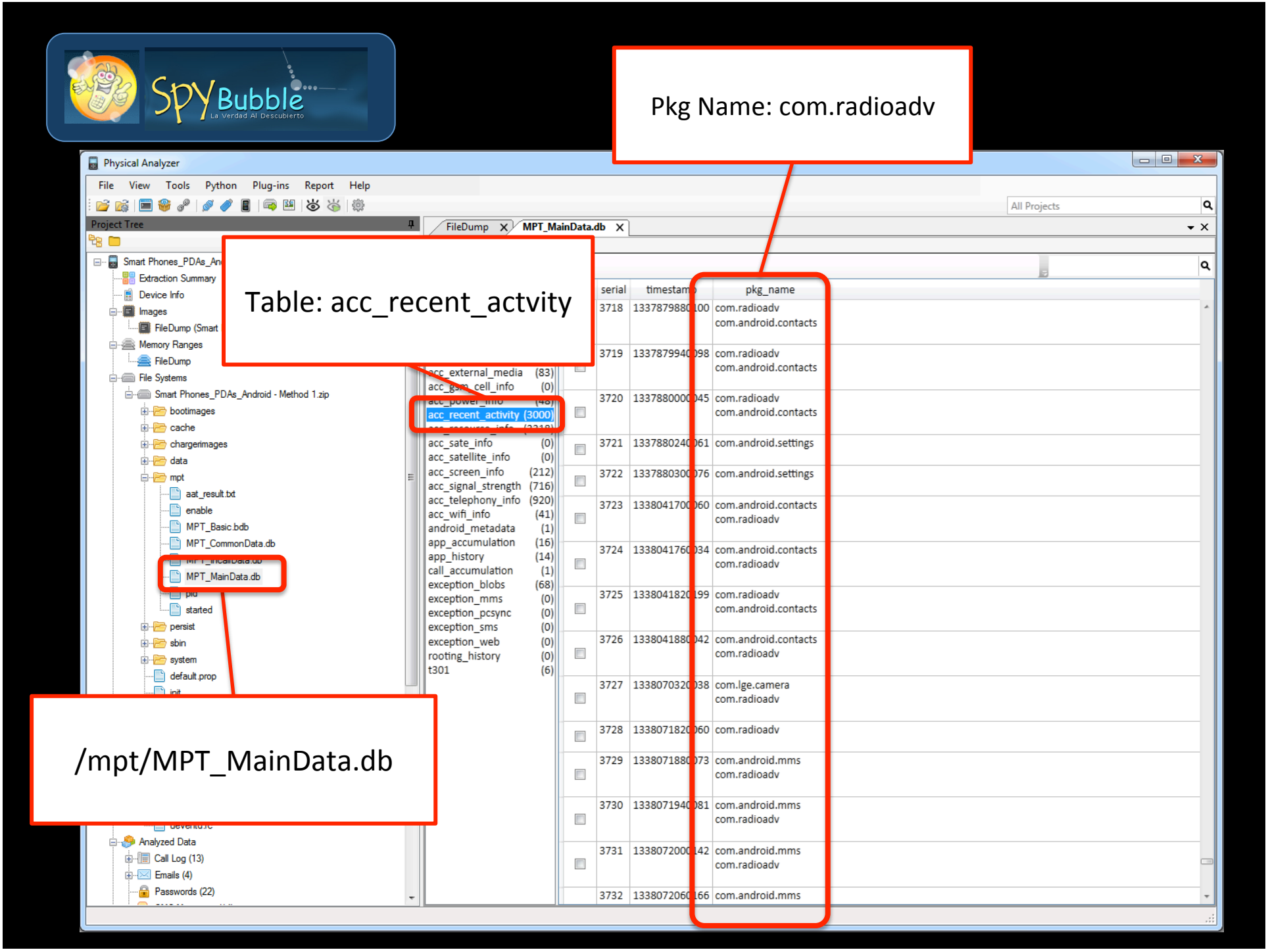
The phone was in my pocket.
Not that useful.

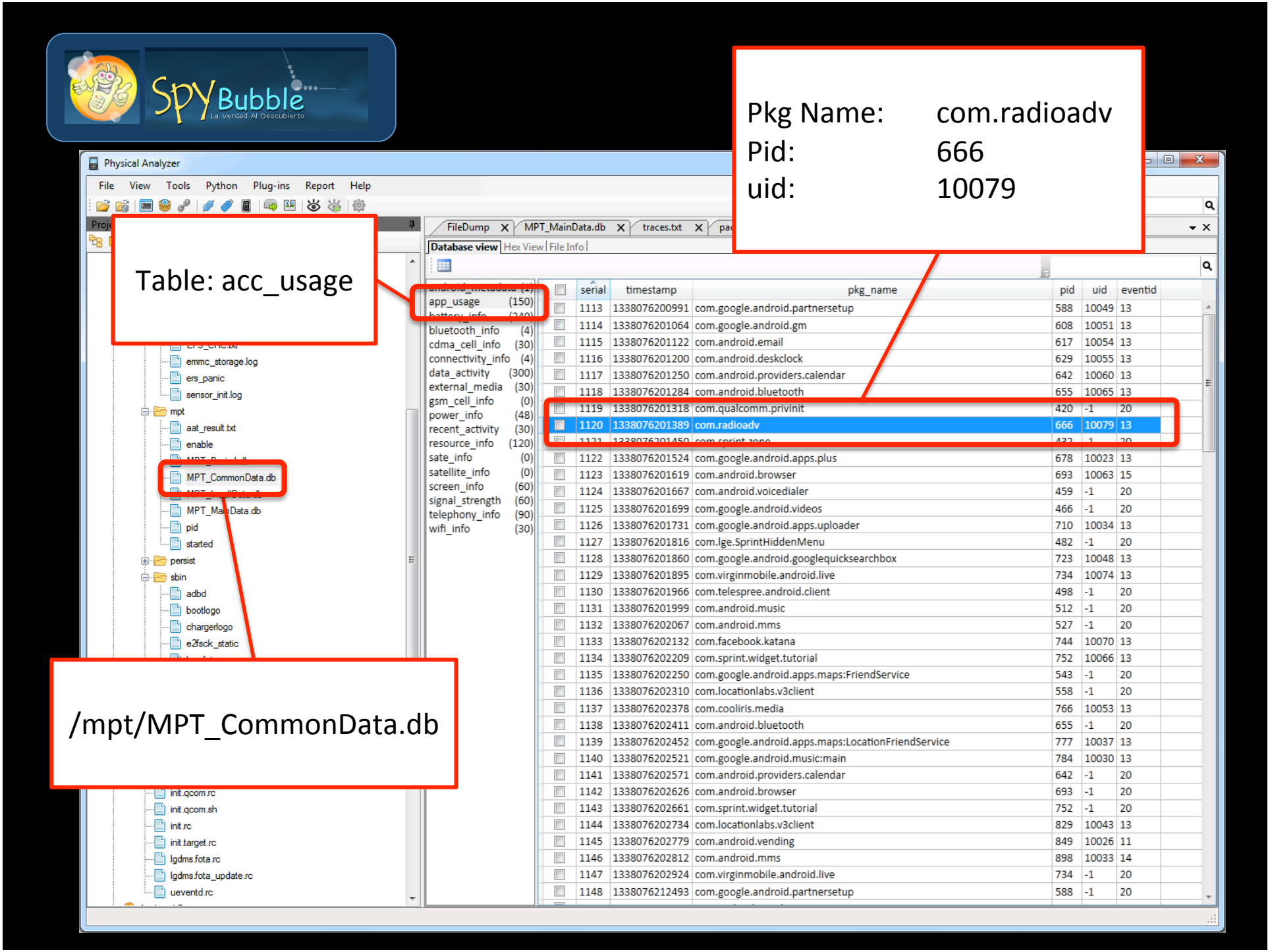
The phone was in my hand.
The raw photo does not focus.


SpyBubble
La Verdad Al Descubierto
Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
Smart Phones_PDAs_Android - Method 1
Extraction Summary
Device Info
Images
FileDump (Smart
Memory Ranges
FileDump
File Systems
Smart Phones_P
bootimages
cache
chargerimages
data
mpt
aat_result.txt
enable
MPT_Basic.bdb
MPT_CommonData.db
MPT_MainData.db
started
persist
sbin
system
default.prop
init
Analyzed Data
Call Log (13)
Emails (4)
Passwords (22)
FileDump
MPT_MainData.db
Database view
Hex View
File Info
acc_recent_activity (3000)
acc_resource_info (3318)
acc_sate_info (0)
acc_satellite_info (0)
acc_screen_info (212)
acc_signal_strength (716)
acc_telephony_info (920)
acc_wifi_info (41)
android_metadata (1)
app_accumulation (16)
app_history (14)
exception_blobs (68)
exception_pcsync (0)
exception_sms (0)
exception_web (0)
rooting_history (0)
t301 (6)
timestamp
1337649765390
1337658471245
FATAL EXCEPTION: main
java.lang.NullPointerException
at com.radioadv.CameraActivity$Preview.surfaceChanged(CameraActivity.java:132)
at android.view.SurfaceView.dispatchDraw(SurfaceView.java:350)
at android.view.ViewGroup.drawChild(ViewGroup.java:1644)
at android.view.ViewGroup.dispatchDraw(ViewGroup.java:1373)
at android.view.View.draw(View.java:6902)
at android.widget.FrameLayout.draw(FrameLayout.java:357)
at android.view.ViewGroup.drawChild(ViewGroup.java:1646)
at android.view.ViewGroup.dispatchDraw(ViewGroup.java:1373)
at android.view.ViewGroup.drawChild(ViewGroup.java:1644)
at android.view.ViewGroup.dispatchDraw(ViewGroup.java:1373)
at android.view.View.draw(View.java:6902)
at android.widget.FrameLayout.draw(FrameLayout.java:357)
at com.android.internal.policy.impl.PhoneWindow$DecorView.draw(PhoneWindow.java:2038)
at android.view.ViewRoot.draw(ViewRoot.java:1527)
at android.view.ViewRoot.performTraversals(ViewRoot.java:1263)
at android.view.ViewRoot.handleMessage(ViewRoot.java:1864)
at android.os.Handler.dispatchMessage(Handler.java:99)
at android.os.Looper.loop(Looper.java:130)
at android.app.ActivityThread.main(ActivityThread.java:3683)
at java.lang.reflect.Method.invokeNative(Native Method)
at java.lang.reflect.Method.invoke(Method.java:507)
at com.android.internal.os.ZygoteInit$MethodAndArgsCaller.run(ZygoteInit.java:875)
at com.android.internal.os.ZygoteInit.main(ZygoteInit.java:633)
at dalvik.system.NativeStart.main(Native Method)
1337665673922
FATAL EXCEPTION: main
java.lang.NullPointerException
at com.radioadv.CameraActivity$Preview.surfaceChanged(CameraActivity.java:132)
at android.view.SurfaceView.updateWindow(SurfaceView.java:558)
at android.view.SurfaceView.dispatchDraw(SurfaceView.java:350)
at android.view.ViewGroup.drawChild(ViewGroup.java:1644)
at android.view.ViewGroup.dispatchDraw(ViewGroup.java:1373)
at android.view.View.draw(View.java:6902)
at android.widget.FrameLayout.draw(FrameLayout.java:357)
at android.view.ViewGroup.drawChild(ViewGroup.java:1646)
at android.view.ViewGroup.dispatchDraw(ViewGroup.java:1373)
at android.view.ViewGroup.drawChild(ViewGroup.java:1644)
com.radioadv.CameraActivity $Preview.surfaceChanged (CameraActivity.java:132)
Table: exception_blobs
/mpt/MPT_MainData.db


SpyBubble
La Verdad Al Descubierto
ANR in com.radioadv
Reason: Executing service com.radioadv/.LivePicService
Load: 12.16/16.72/15.64
CPU usage from16515ms to 0ms ago:
1% 4261/com.radioadv: 1% user + 0% kernel / faults: 145 minor
Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
FileDump
Database view
Smart Phones_PDAs_Android - Method 1
Extraction Summary
Device Info
Images
FileDump (Smart
Memory Ranges
FileDump
File Systems
Smart Phones_P
bootimages
cache
chargerimages
data
mpt
aat_result.txt
enable
MPT_Basic.bdb
MPT_CommonData.db
MPT_MainData.db
started
persist
sbin
system
default.prop
init
Analyzed Data
Call Log (13)
Emails (4)
Passwords (22)
acc_recent_activity (3000)
acc_resource_info (3318)
acc_sate_info (0)
acc_satellite_info (0)
acc_screen_info (212)
acc_signal_strength (716)
acc_telephony_info (920)
acc_wifi_info (41)
android_metadata (1)
app_accumulation (16)
app_history (14)
call_accumulation (1)
exception_blobs (68)
exception_pcsync (0)
exception_sms (0)
exception_web (0)
rooting_history (0)
t301 (6)
timestamp
133779582878
ANR in com.radioadv
Reason: Executing service com.radioadv/.LivePicService
Load: 12.16 / 16.72 / 15.64
CPU usage from 16515ms to 0ms ago:
2.6% 4532/mediaserver: 1.8% user + 0.7% kernel
1% 4261/com.radioadv: 1% user + 0% kernel / faults: 145 minor
0.5% 2283/com.lge.mlt: 0.4% user + 0.1% kernel / faults: 59 minor
0.4% 202/system_server: 0.2% user + 0.1% kernel / faults: 3 minor
0.2% 78/mmcqd: 0% user + 0.2% kernel
0.1% 331/MC_Thread: 0% user + 0.1% kernel
0% 329/ksdioirqd/mmc1: 0% user + 0% kernel
0% 1//init: 0% user + 0% kernel / faults: 16 minor
0% 66/kondemand/0: 0% user + 0% kernel
0% 105/jbd2/mmcblk0p21: 0% user + 0% kernel
0% 287/com.android.phone: 0% user + 0% kernel / faults: 1 minor
0% 332/TX_Thread: 0% user + 0% kernel
0% 361/wpa_supplicant: 0% user + 0% kernel
0% 2299/logcat: 0% user + 0% kernel
4.4% TOTAL: 2.9% user + 0.8% kernel + 0.6% iowait
CPU usage from 738ms to 1251ms later:
3.9% 202/system_server: 0% user + 3.9% kernel / faults: 1 minor
1.9% 229/ActivityManager: 0% user + 1.9% kernel
1.6% 4532/mediaserver: 1.6% user + 0% kernel
1.6% 5109/AudioTrackEncod: 1.6% user + 0% kernel
5.7% TOTAL: 1.9% user + 3.8% kernel
FATAL EXCEPTION: main
java.lang.NullPointerException
at com.radioadv.CameraActivity$Preview.surfaceChanged(CameraActivity.java:132)
at android.view.SurfaceView.updateWindow(SurfaceView.java:558)
at android.view.SurfaceView.dispatchDraw(SurfaceView.java:350)
at android.view.ViewGroup.drawChild(ViewGroup.java:1644)
at android.view.ViewGroup.dispatchDraw(ViewGroup.java:1373)
at android.view.View.draw(View.java:6902)
at android.widget.FrameLayout.draw(FrameLayout.java:357)
at android.view.ViewGroup.drawChild(ViewGroup.java:1646)
at android.view.ViewGroup.dispatchDraw(ViewGroup.java:1373)
at android.view.ViewGroup.drawChild(ViewGroup.java:1644)
at android.view.ViewGroup.dispatchDraw(ViewGroup.java:1373)
at android.view.View.draw(View.java:6902)
at android.widget.FrameLayout.draw(FrameLayout.java:357)
Table: exception_blobs
/mpt/MPT_MainData.db


SpyBubble
La Verdad Al Descubierto
Mon May 21 2012 20:48:27 GMT-0400 (EDT)
Pkg Name: com.radioadv
Install Time: 1337647707115
Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
Smart Phones_PDAs_Android - Method 1
Extraction Summary
Device Info
Images
FileDump (Smart Phones_PDAs_Android - Method 1.zip)
Memory Ranges
FileDump
File Systems
Smart Phones_PDAs_And
bootimages
cache
chargerimages
data
mpt
aat_result.txt
enable
MPT_Basic.bdb
MPT_CommonData.db
MPT_MainData.db
started
persist
sbin
system
default.prop
init
Analyzed Data
Call Log (13)
Emails (4)
Passwords (22)
FileDump
Database view
Hex View
File Info
acc_app_usage (1262)
acc_battery_info (747)
acc_bluetooth_info (4)
acc_cdma_cell_info (543)
acc_signal_strength (716)
acc_telephony_info (920)
acc_wifi_info (41)
android_metadata (1)
app_history (14)
exception_blobs (68)
exception_mms (0)
exception_pcsync (0)
exception_sms (0)
exception_web (0)
rooting_history (0)
t301 (6)
serial timestamp pkg_name install_time delete_time last_version
1 1337626373965 com.sprint.sprintid.appstub 1337626373965 0 1
2 1337626376487 com.buzzfeed.android 1337626376487 0 1.7
3 1337626381687 com.facebook.katana 1337626381687 0 1.6
4 1337626382664 com.yelp.android 1337626382664 0 0
5 1337626383799 com.markus.tuningfork 1337626383799 0 3
6 1337626384776 com.vmobile.iconpack 1337626384776 0 1.1
7 1337626386662 com.virginmobile.android.live 1337626386662 0 1.01
8 1337626388796 com.virginmobileusa.vmlive 1337626388796 0 0.6
9 1337626389846 com.cellmania.android.storefront.webview.vmu 1337626389846 0 2
10 1337626391476 org.wikipedia 1337626391476 0 1
12 1337647707115 com.radioadv 1337647707115 0 1
14 1338123738531 com.android.vending 1338123738262 0 3.5
Table: app_history
/mpt/MPT_MainData.db


SpyBubble
La Verdad Al Descubierto
Pkg Name: com.radioadv
Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
FileDump
MPT_MainData.db
Table: acc_recent_actvity
acc_recent_activity (3000)
serial
pkg_name
com.radioadv
com.android.contacts
com.android.settings
com.android.mms
com.lge.camera
/mpt/MPT_MainData.db



serial	timestamp	pkg_name	pid	uid	eventid
1113	1338076200991	com.google.android.partnersetup	588	10049	13
1114	1338076201064	com.google.android.gm	608	10051	13
1115	1338076201122	com.android.email	617	10054	13
1116	1338076201200	com.android.deskclock	629	10055	13
1117	1338076201250	com.android.providers.calendar	642	10060	13
1118	1338076201284	com.android.bluetooth	655	10065	13
1119	1338076201318	com.qualcomm.privinit	420	-1	20
1120	1338076201389	com.radioadv	666	10079	13
1122	1338076201524	com.google.android.apps.plus	678	10023	13
1123	1338076201619	com.android.browser	693	10063	15
1124	1338076201667	com.android.voicedialer	459	-1	20
1125	1338076201699	com.google.android.videos	466	-1	20
1126	1338076201731	com.google.android.apps.uploader	710	10034	13
1127	1338076201816	com.lge.SprintHiddenMenu	482	-1	20
1128	1338076201860	com.google.android.googlequicksearchbox	723	10048	13
1129	1338076201895	com.virginmobile.android.live	734	10074	13
1130	1338076201966	com.telespree.android.client	498	-1	20
1131	1338076201999	com.android.music	512	-1	20
1132	1338076202067	com.android.mms	527	-1	20
1133	1338076202132	com.facebook.katana	744	10070	13
1134	1338076202209	com.sprint.widget.tutorial	752	10066	13
1135	1338076202250	com.google.android.apps.maps:FriendService	543	-1	20
1136	1338076202310	com.locationlabs.v3client	558	-1	20
1137	1338076202378	com.cooliris.media	766	10053	13
1138	1338076202411	com.android.bluetooth	655	-1	20
1139	1338076202452	com.google.android.apps.maps:LocationFriendService	777	10037	13
1140	1338076202521	com.google.android.music:main	784	10030	13
1141	1338076202571	com.android.providers.calendar	642	-1	20
1142	1338076202626	com.android.browser	693	-1	20
1143	1338076202661	com.sprint.widget.tutorial	752	-1	20
1144	1338076202734	com.locationlabs.v3client	829	10043	13
1145	1338076202779	com.android.vending	849	10026	11
1146	1338076202812	com.android.mms	898	10033	14
1147	1338076202924	com.virginmobile.android.live	734	-1	20
1148	1338076212493	com.google.android.partnersetup	588	-1	20


Mobistealth

URL history

http://www.mobistealth.com/asset/mobistealthv2.apk

downloads.db entry

uri: http://www.mobistealth.com/asset/mobistealthv2.apk

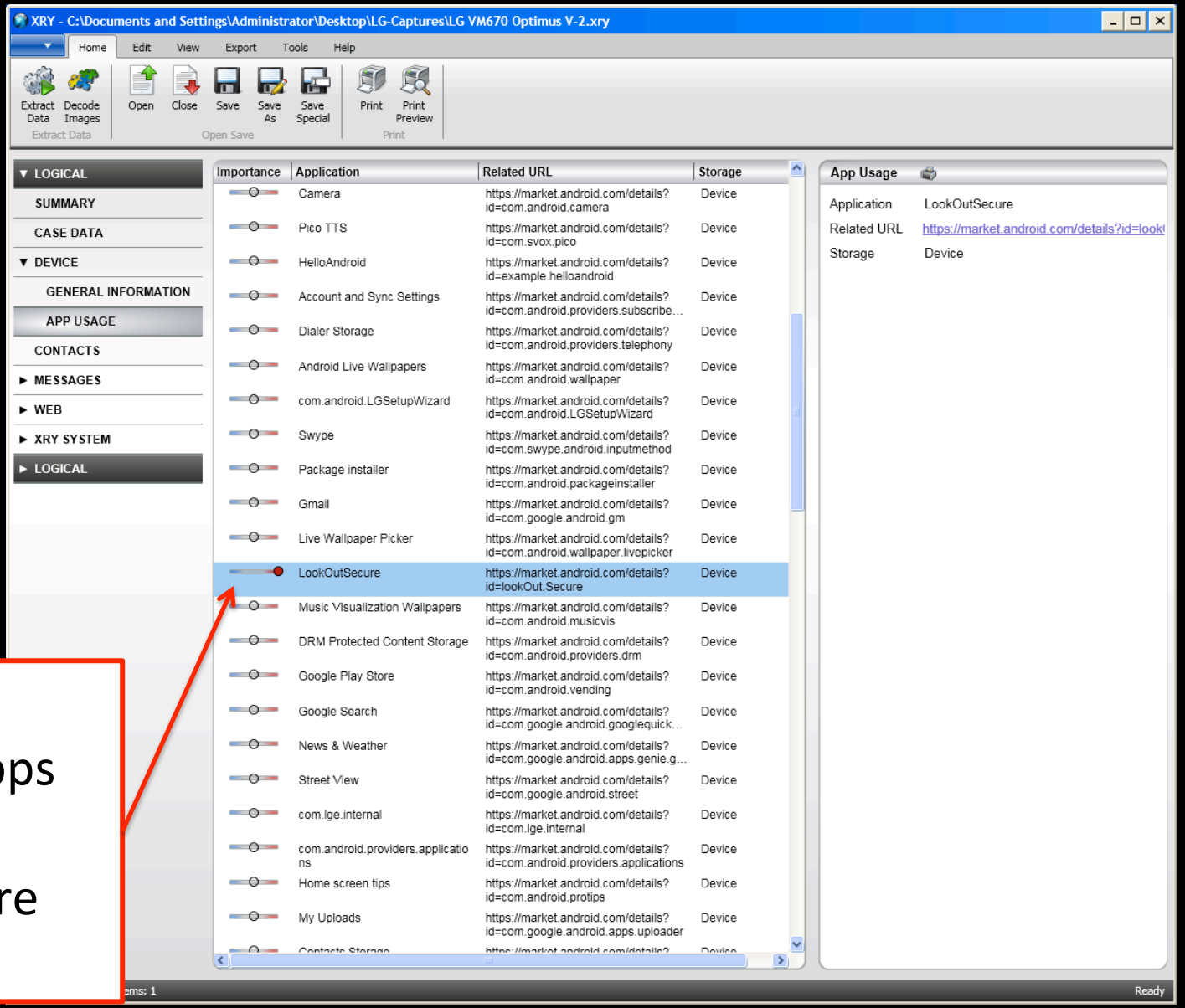
Hint: mobistealthv2.apk

_data: /mnt/sdcard/download/mobistealthv2.apk

SD Card

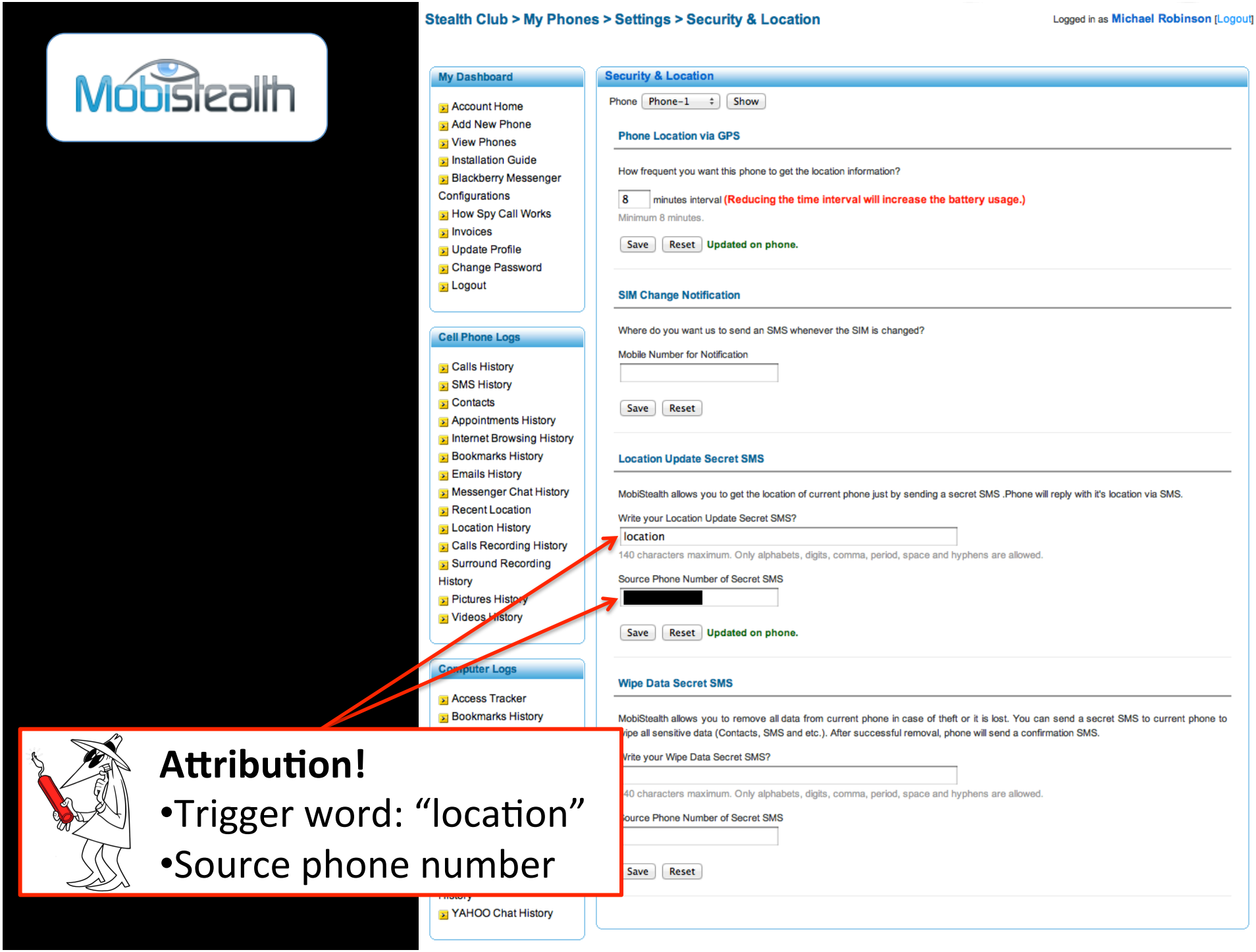
\download\mobistealthv2.apk

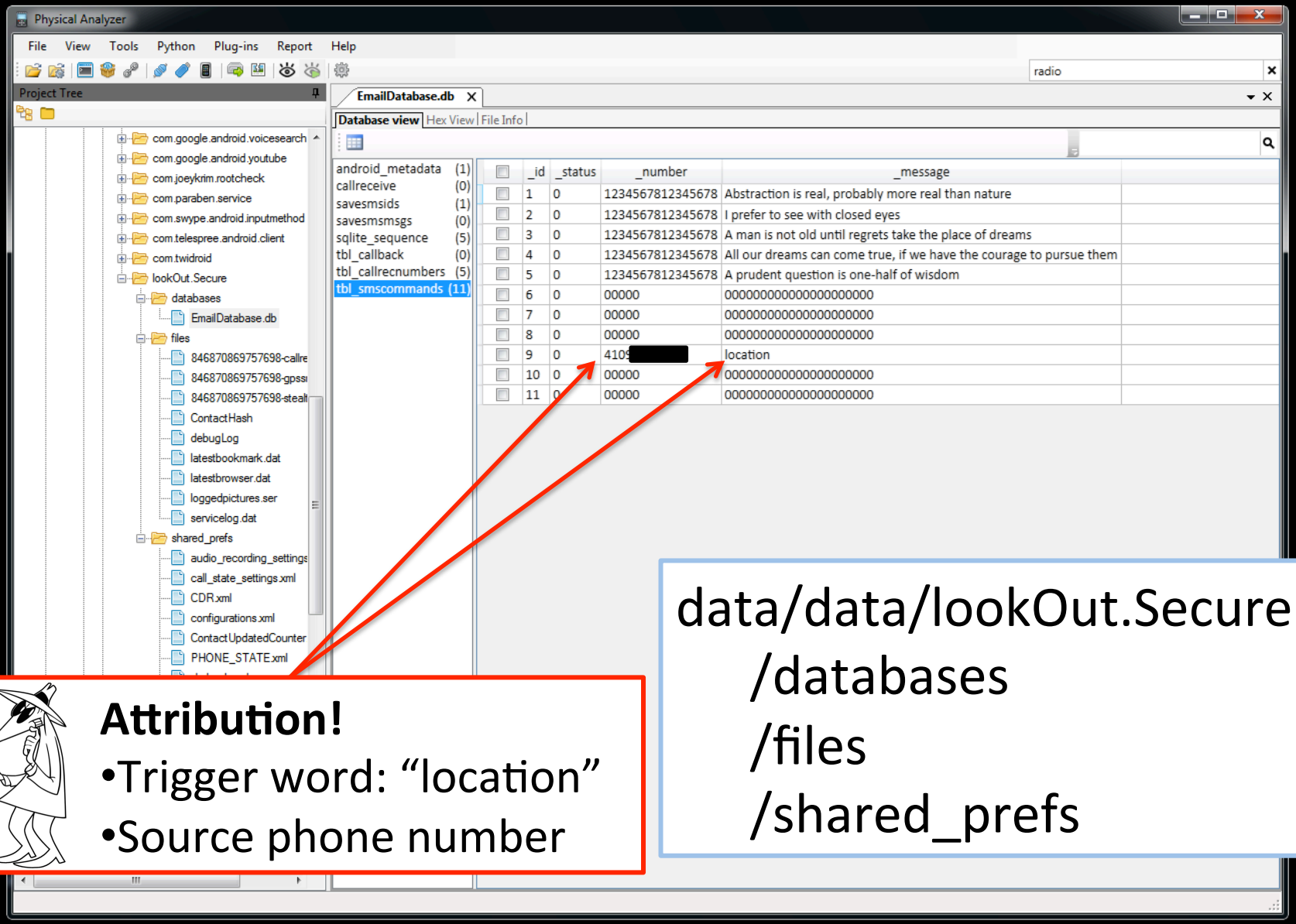
Mobistealth



84 Running Apps

LookOutSecure

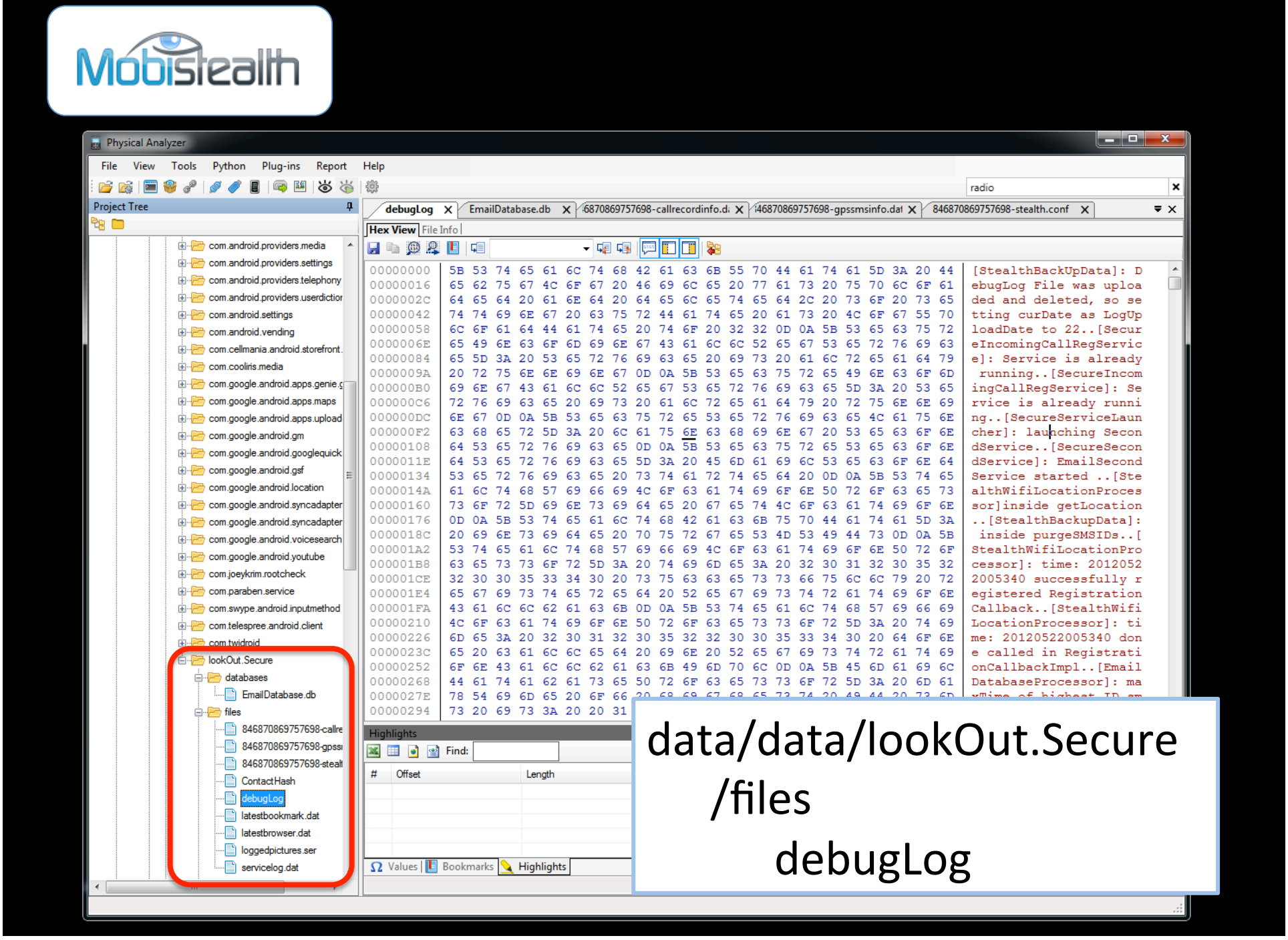

Stealth Club > My Phones > Settings > Security & Location
Logged in as Michael Robinson [Logout]
My Dashboard
Account Home
Add New Phone
View Phones
Installation Guide
Blackberry Messenger Configurations
How Spy Call Works
Invoices
Update Profile
Change Password
Logout
Cell Phone Logs
Calls History
SMS History
Contacts
Appointments History
Internet Browsing History
Bookmarks History
Emails History
Messenger Chat History
Recent Location
Location History
Calls Recording History
Surround Recording History
Pictures History
Videos History
Computer Logs
Access Tracker
Bookmarks History
YAHOO Chat History
Security & Location
Phone Phone-1 Show
Phone Location via GPS
How frequent you want this phone to get the location information?
8 minutes interval (Reducing the time interval will increase the battery usage.)
Minimum 8 minutes.
Save Reset Updated on phone.
SIM Change Notification
Where do you want us to send an SMS whenever the SIM is changed?
Mobile Number for Notification
Save Reset
Location Update Secret SMS
MobiStealth allows you to get the location of current phone just by sending a secret SMS .Phone will reply with it's location via SMS.
Write your Location Update Secret SMS?
location
140 characters maximum. Only alphabets, digits, comma, period, space and hyphens are allowed.
Source Phone Number of Secret SMS
[redacted]
Save Reset Updated on phone.
Wipe Data Secret SMS
MobiStealth allows you to remove all data from current phone in case of theft or it is lost. You can send a secret SMS to current phone to wipe all sensitive data (Contacts, SMS and etc.). After successful removal, phone will send a confirmation SMS.
Write your Wipe Data Secret SMS?
140 characters maximum. Only alphabets, digits, comma, period, space and hyphens are allowed.
Source Phone Number of Secret SMS
Save Reset
Attribution!
•Trigger word: “location”
•Source phone number

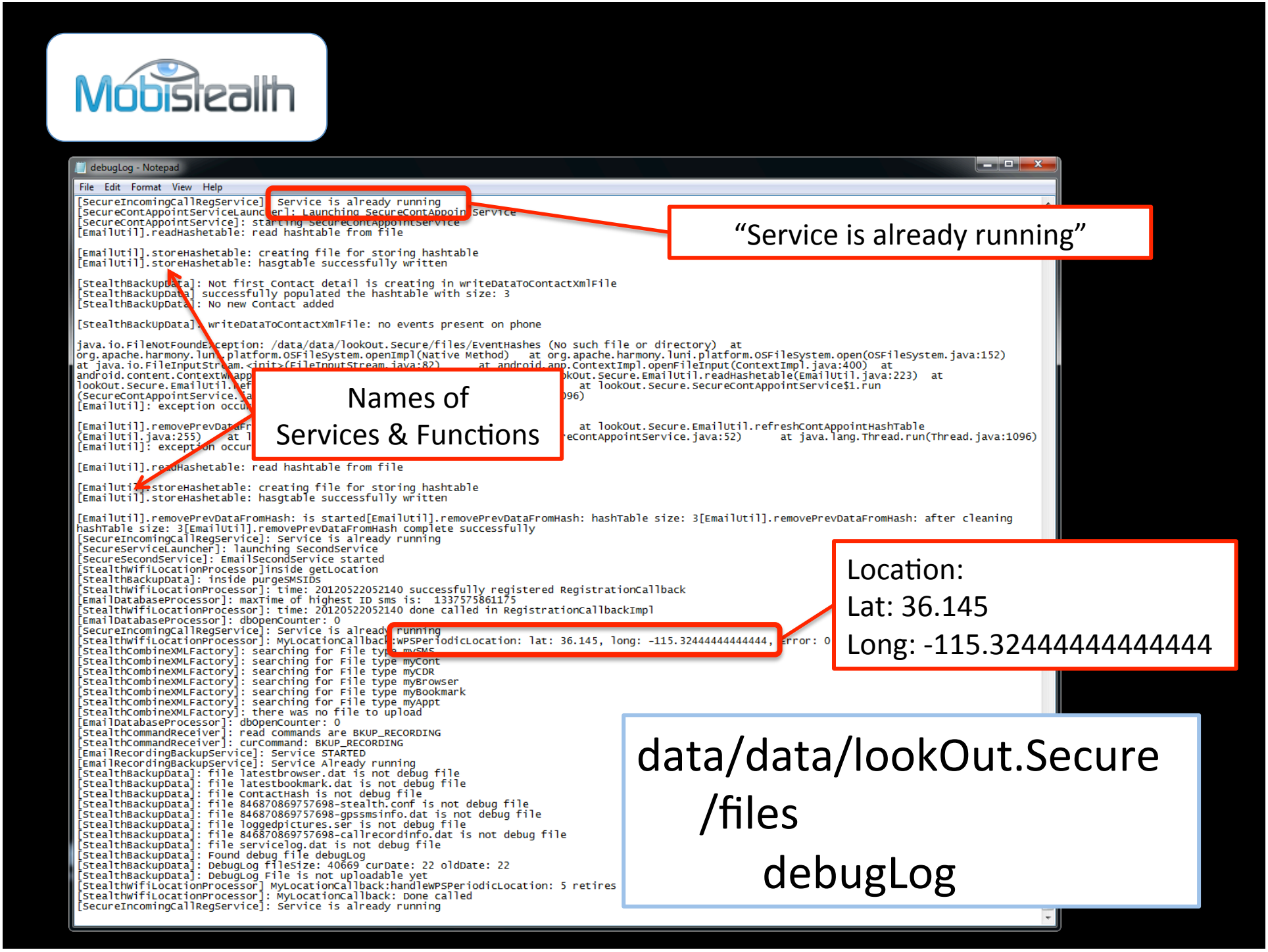


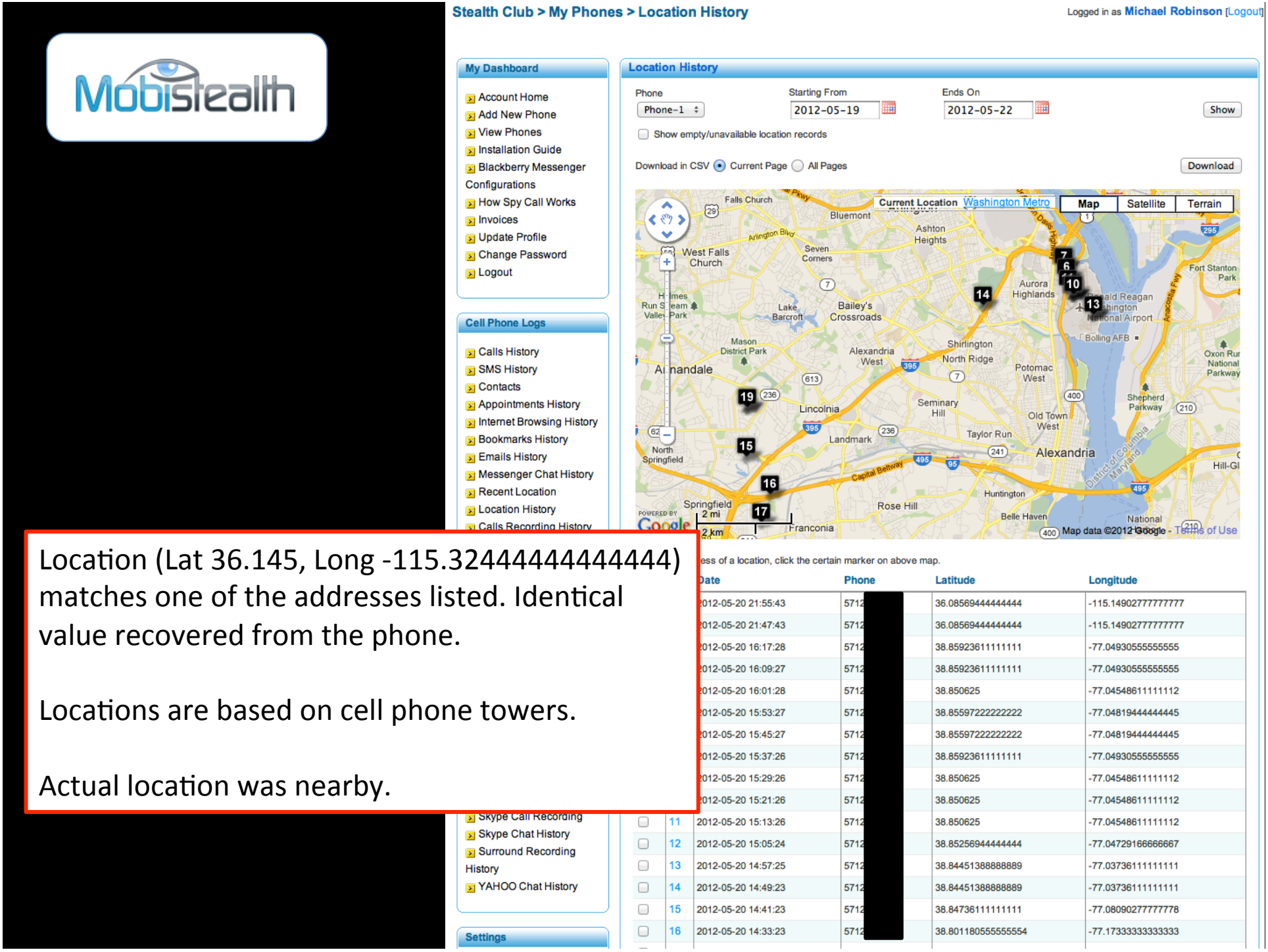
Attribution!

- Trigger word: “location”
- Source phone number

data/data/lookOut.Secure
/databases
/files
/shared_prefs

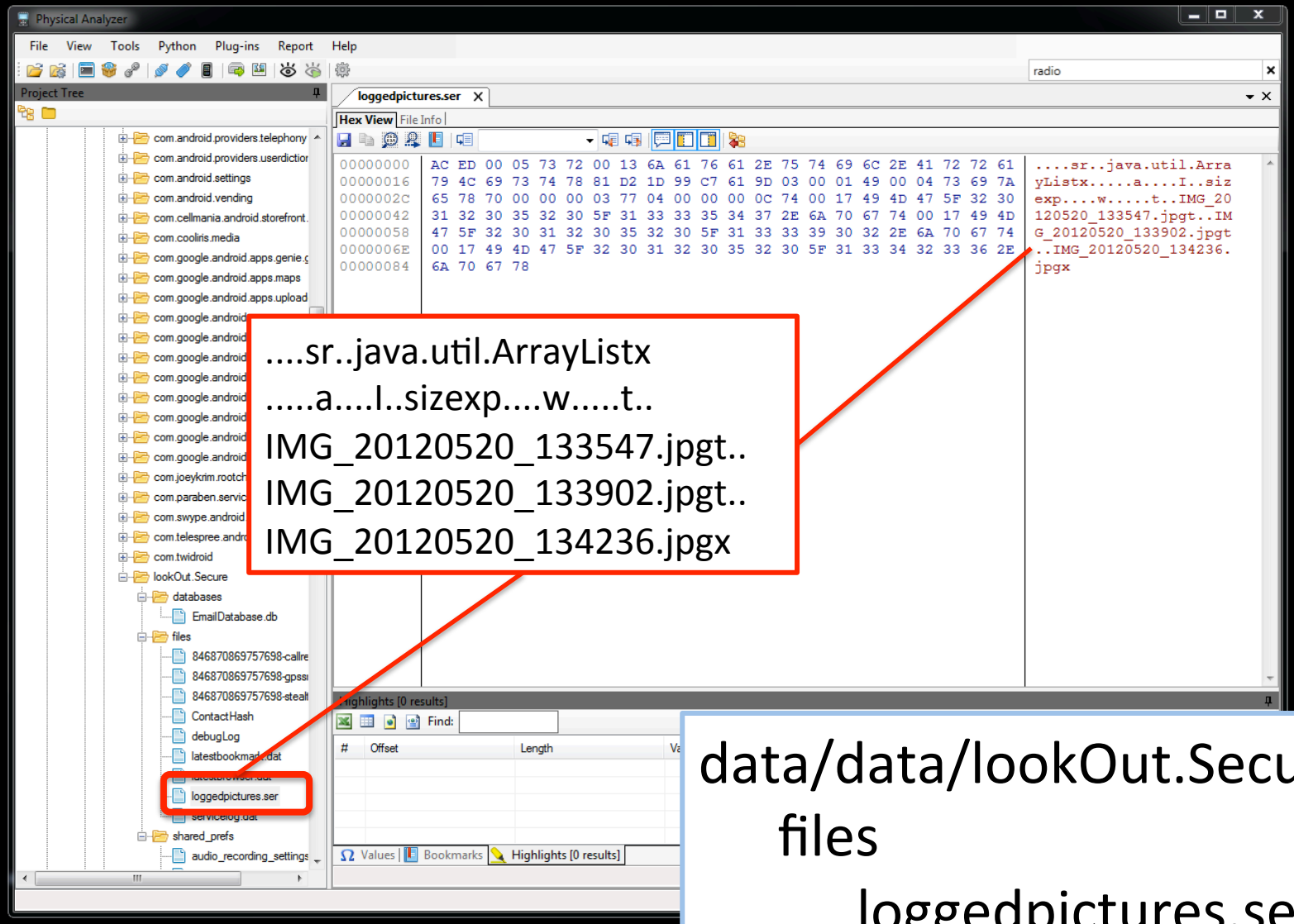

Physical Analyzer
File View Tools Python Plug-ins Report Help
Project Tree
debugLog
EmailDatabase.db
Hex View
File Info
lookOut.Secure
databases
EmailDatabase.db
files
ContactHash
debugLog
latestbookmark.dat
latestbrowser.dat
loggedpictures.ser
servicelog.dat
Highlights
Find:
Offset
Length
Values
Bookmarks
Highlights
data/data/lookOut.Secure
/files
debugLog


Mobistealth
debugLog - Notepad
File Edit Format View Help
[SecureIncomingCallRegService]: Service is already running
[SecureContAppointServiceLauncher]: Launching SecureContAppointService
[SecureContAppointService]: starting SecureContAppointService
[EmailUtil].readHashetable: read hashtable from file
[EmailUtil].storeHashetable: creating file for storing hashtable
[EmailUtil].storeHashetable: hasgtable successfully written
[StealthBackUpData]: Not first Contact detail is creating in writeDataToContactXmlFile
[StealthBackUpData] successfully populated the hashtable with size: 3
[StealthBackUpData]: No new Contact added
[StealthBackUpData]: writeDataToContactXmlFile: no events present on phone
java.io.FileNotFoundException: /data/data/lookOut.Secure/files/EventHashes (No such file or directory) at
org.apache.harmony.luni.platform.OSFileSystem.openImpl(Native Method) at org.apache.harmony.luni.platform.OSFileSystem.open(OSFileSystem.java:152)
at java.io.FileInputStream.<init>(FileInputStream.java:82) at android.app.ContextImpl.openFileInput(ContextImpl.java:400) at
android.content.ContextWrapper
lookOut.Secure.EmailUtil.readHashetable(EmailUtil.java:223) at
lookOut.Secure.EmailUtil.ref
at lookOut.Secure.SecureContAppointService$1.run
(SecureContAppointService.ja
096)
[EmailUtil]: exception occu
[EmailUtil].removePrevDataFr
at lookOut.Secure.EmailUtil.refreshContAppointHashTable
(EmailUtil.java:255) at l
reContAppointService.java:52) at java.lang.Thread.run(Thread.java:1096)
[EmailUtil]: exception occur
[EmailUtil].readHashetable: read hashtable from file
[EmailUtil].storeHashetable: creating file for storing hashtable
[EmailUtil].storeHashetable: hasgtable successfully written
[EmailUtil].removePrevDataFromHash: is started[EmailUtil].removePrevDataFromHash: hashTable size: 3[EmailUtil].removePrevDataFromHash: after cleaning
hashTable size: 3[EmailUtil].removePrevDataFromHash complete successfully
[SecureIncomingCallRegService]: Service is already running
[SecureServiceLauncher]: launching SecondService
[SecureSecondService]: EmailSecondService started
[StealthWifiLocationProcessor]inside getLocation
[StealthBackupData]: inside purgeSMSIDs
[StealthWifiLocationProcessor]: time: 20120522052140 successfully registered RegistrationCallback
[EmailDatabaseProcessor]: maxTime of highest ID sms is: 1337575861175
[StealthWifiLocationProcessor]: time: 20120522052140 done called in RegistrationCallbackImpl
[EmailDatabaseProcessor]: dbOpenCounter: 0
[SecureIncomingCallRegService]: Service is already running
[StealthWifiLocationProcessor]: MyLocationCallback:WPSPeriodicLocation: lat: 36.145, long: -115.32444444444444, error: 0
[StealthCombineXMLFactory]: searching for File type mySMS
[StealthCombineXMLFactory]: searching for File type myCont
[StealthCombineXMLFactory]: searching for File type myCDR
[StealthCombineXMLFactory]: searching for File type myBrowser
[StealthCombineXMLFactory]: searching for File type myBookmark
[StealthCombineXMLFactory]: searching for File type myAppt
[StealthCombineXMLFactory]: there was no file to upload
[EmailDatabaseProcessor]: dbOpenCounter: 0
[StealthCommandReceiver]: read commands are BKUP_RECORDING
[StealthCommandReceiver]: curCommand: BKUP_RECORDING
[EmailRecordingBackupService]: Service STARTED
[EmailRecordingBackupService]: Service Already running
[StealthBackupData]: file latestbrowser.dat is not debug file
[StealthBackupData]: file latestbookmark.dat is not debug file
[StealthBackupData]: file ContactHash is not debug file
[StealthBackupData]: file 846870869757698-stealth.conf is not debug file
[StealthBackupData]: file 846870869757698-gpssmsinfo.dat is not debug file
[StealthBackupData]: file loggedpictures.ser is not debug file
[StealthBackupData]: file 846870869757698-callrecordinfo.dat is not debug file
[StealthBackupData]: file servicelog.dat is not debug file
[StealthBackupData]: Found debug file debugLog
[StealthBackupData]: DebugLog fileSize: 40669 curDate: 22 oldDate: 22
[StealthBackupData]: DebugLog File is not uploadable yet
[StealthWifiLocationProcessor] MyLocationCallback:handleWPSPeriodicLocation: 5 retires
[StealthWifiLocationProcessor]: MyLocationCallback: Done called
[SecureIncomingCallRegService]: Service is already running
“Service is already running”
Names of
Services & Functions
Location:
Lat: 36.145
Long: -115.32444444444444
data/data/lookOut.Secure
/files
debugLog



		Date	Phone	Latitude	Longitude
		2012-05-20 21:55:43	5712[redacted]	36.08569444444444	-115.14902777777777
		2012-05-20 21:47:43	5712[redacted]	36.08569444444444	-115.14902777777777
		2012-05-20 16:17:28	5712[redacted]	38.85923611111111	-77.04930555555555
		2012-05-20 16:09:27	5712[redacted]	38.85923611111111	-77.04930555555555
		2012-05-20 16:01:28	5712[redacted]	38.850625	-77.04548611111112
		2012-05-20 15:53:27	5712[redacted]	38.85597222222222	-77.04819444444445
		2012-05-20 15:45:27	5712[redacted]	38.85597222222222	-77.04819444444445
		2012-05-20 15:37:26	5712[redacted]	38.85923611111111	-77.04930555555555
		2012-05-20 15:29:26	5712[redacted]	38.850625	-77.04548611111112
		2012-05-20 15:21:26	5712[redacted]	38.850625	-77.04548611111112
	11	2012-05-20 15:13:26	5712[redacted]	38.850625	-77.04548611111112
	12	2012-05-20 15:05:24	5712[redacted]	38.85256944444444	-77.04729166666667
	13	2012-05-20 14:57:25	5712[redacted]	38.84451388888889	-77.03736111111111
	14	2012-05-20 14:49:23	5712[redacted]	38.84451388888889	-77.03736111111111
	15	2012-05-20 14:41:23	5712[redacted]	38.84736111111111	-77.08090277777778
	16	2012-05-20 14:33:23	5712[redacted]	38.801180555555554	-77.17333333333333

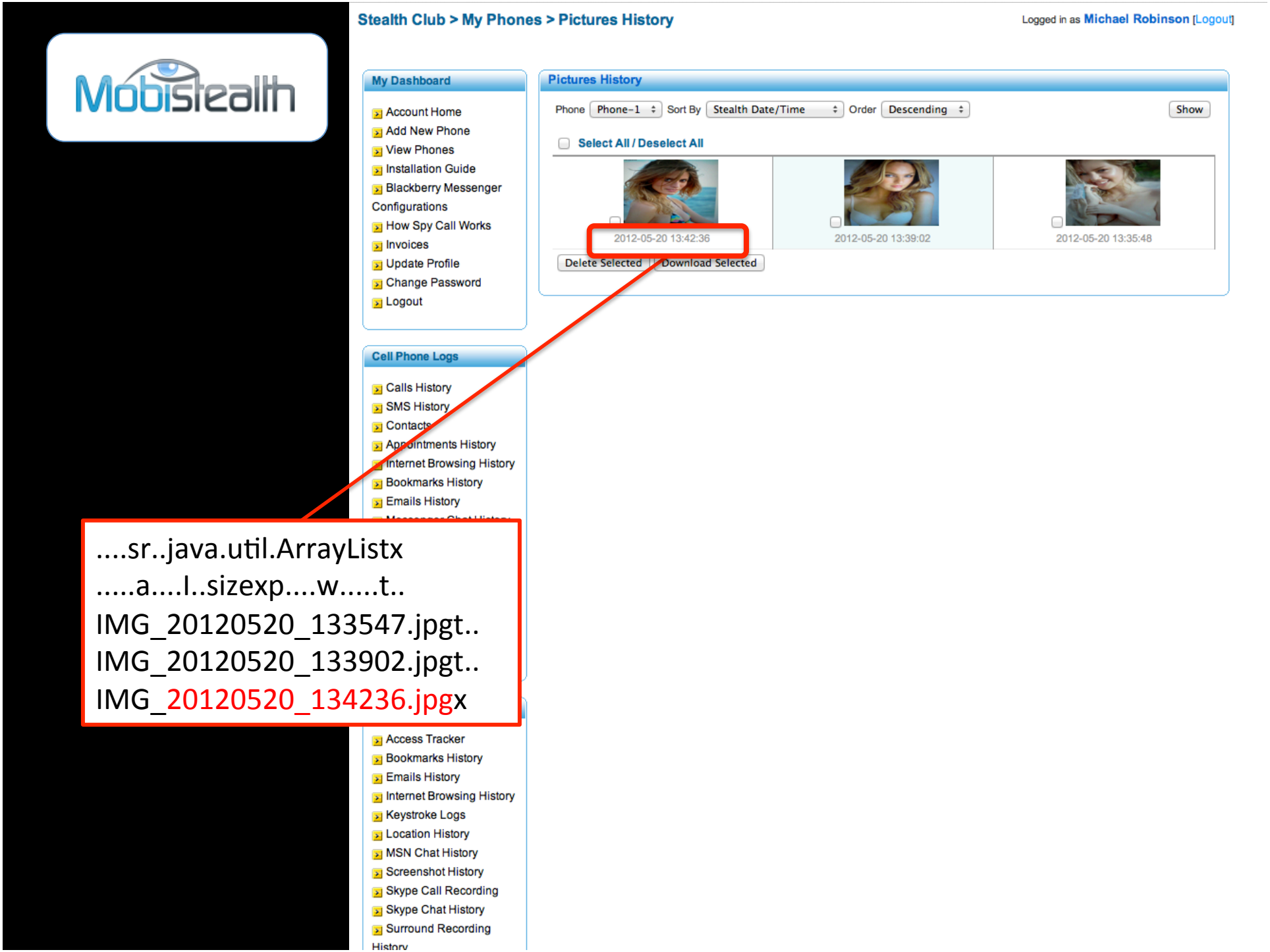
List of pictures that have been uploaded.

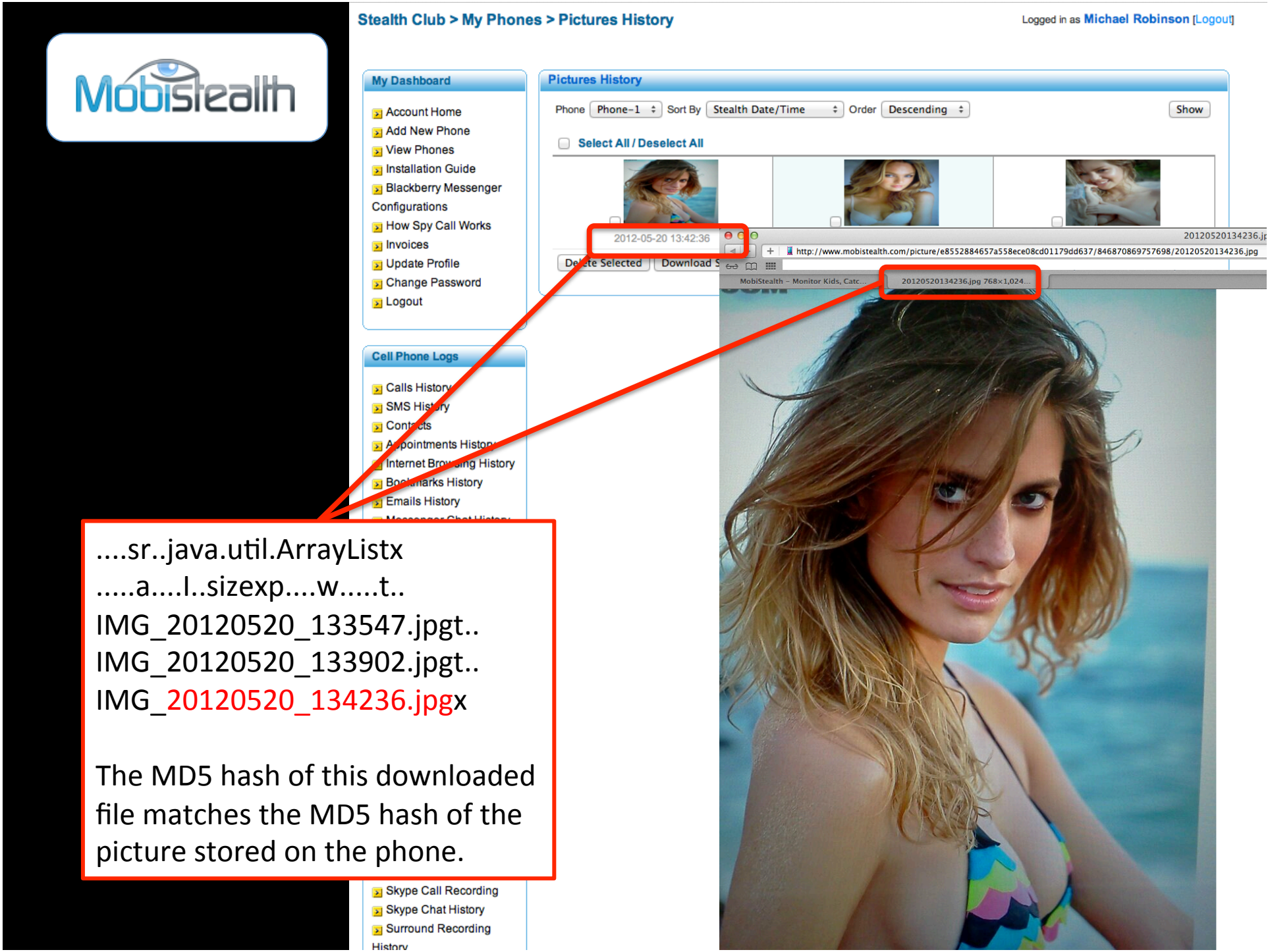


data/data/lookOut.Secure

files

loggedpictures.ser


Stealth Club > My Phones > Pictures History
Logged in as Michael Robinson [Logout]
My Dashboard
Account Home
Add New Phone
View Phones
Installation Guide
Blackberry Messenger Configurations
How Spy Call Works
Invoices
Update Profile
Change Password
Logout
Cell Phone Logs
Calls History
SMS History
Contacts
Appointments History
Internet Browsing History
Bookmarks History
Emails History
Access Tracker
Bookmarks History
Emails History
Internet Browsing History
Keystroke Logs
Location History
MSN Chat History
Screenshot History
Skype Call Recording
Skype Chat History
Surround Recording History
Pictures History
Phone Phone-1 Sort By Stealth Date/Time Order Descending Show
Select All / Deselect All
2012-05-20 13:42:36
2012-05-20 13:39:02
2012-05-20 13:35:48
Delete Selected
Download Selected
....sr..java.util.ArrayListx
.....a....I..sizexp....w.....t..
IMG_20120520_133547.jpgt..
IMG_20120520_133902.jpgt..
IMG_20120520_134236.jpgx


Stealth Club > My Phones > Pictures History
Logged in as Michael Robinson [Logout]
My Dashboard
Account Home
Add New Phone
View Phones
Installation Guide
Blackberry Messenger Configurations
How Spy Call Works
Invoices
Update Profile
Change Password
Logout
Cell Phone Logs
Calls History
SMS History
Contacts
Appointments History
Internet Browsing History
Bookmarks History
Emails History
Skype Call Recording
Skype Chat History
Surround Recording History
Pictures History
Phone Phone-1 Sort By Stealth Date/Time Order Descending Show
Select All / Deselect All
2012-05-20 13:42:36
Delete Selected
Download S
20120520134236.jpg
http://www.mobistealth.com/picture/e8552884657a558ece08cd01179dd637/846870869757698/20120520134236.jpg
MobiStealth – Monitor Kids, Catc...
20120520134236.jpg 768×1,024...
....sr..java.util.ArrayListx
.....a....I..sizexp....w.....t..
IMG_20120520_133547.jpgt..
IMG_20120520_133902.jpgt..
IMG_20120520_134236.jpgx
The MD5 hash of this downloaded file matches the MD5 hash of the picture stored on the phone.

Mobistealth

Physical Analyzer

File View Tools Python Plug-ins Report Help

Project Tree

- com.telespree.android.client
- com.twidroid
- lookOut.Secure
  - databases
    - EmailDatabase.db
  - files
    - 846870869757698-callre
    - 846870869757698-gpssi
    - 846870869757698-stealt
    - ContactHash
    - debugLog
    - latestbookmark.dat
    - latestbrowser.dat
    - loggedpictures.ser
    - servicelog.dat
  - shared_prefs
    - audio_recording_settings
    - call_state_settings.xml
    - configurations.xml
    - PHONE_STATE.xml
    - skyhook.xml
    - SMS.xml
    - sms_backup_pref.xml
- dontpanic
- local
- misc
- property

Hex View | File Info

Untitled - Notepad

File Edit Format View Help

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="app_imei">8468[redacted]</string>
<string name="ftp_rest_passwd">[redacted]</string>
<string name="license_version">Pro-X</string>
<string name="license_status">ACTIVE</string>
<string name="second_service_time">1337689300527</string>
<string name="ftp_port">21</string>
<string name="ftp_init_user">[redacted]</string>
<string name="callrec_mode">STRATEGY_A|MODE_1</string>
<string name="location_interval">8</string>
<string name="ftp_rest_user">mobistealth[redacted]</string>
<string name="local_phone_number">571[redacted]</string>
<string name="ftp_init_passwd">[redacted]</string>
<string name="logupload_date">22</string>
<string name="ftp_server_ip">[redacted]</string>
<boolean name="app_first_launch" value="false" />
<boolean name="app_configuration_created" value="true" />
<string name="ftp_log_user">[redacted]</string>
<string name="ftp_log_passwd">[redacted]</string>
<string name="phone_typ">CDMA</str
<string name="phone_model">VM670<
</map>
```

Source

Length: 0x468 Offset: 0x187 Selection: 0x0

Tue May 22 2012
08:21:40 GMT-0400 (EDT)

Attribution!
FTP credentials
(names and passwords)

/data/data/lookOut.Secure/shared_prefs/configurations.xml
Contents:

- IMEI
- FTP connection information
- CDMA
- Phone Model


MOBILE SPY
Spy Software for
Smartphones

URL history

http://asd-ms.com/ms5-a/ms5-2.1-above.apk

downloads.db entry

uri: http://asd-ms.com/ms5-1/ms5-2.1-above.apk

Hint: ms5-2.1-above.apk

_data: /mnt/sdcard/download/ms5-2.1-above.apk

SD Card

\download\ms5-2.1-above.apk

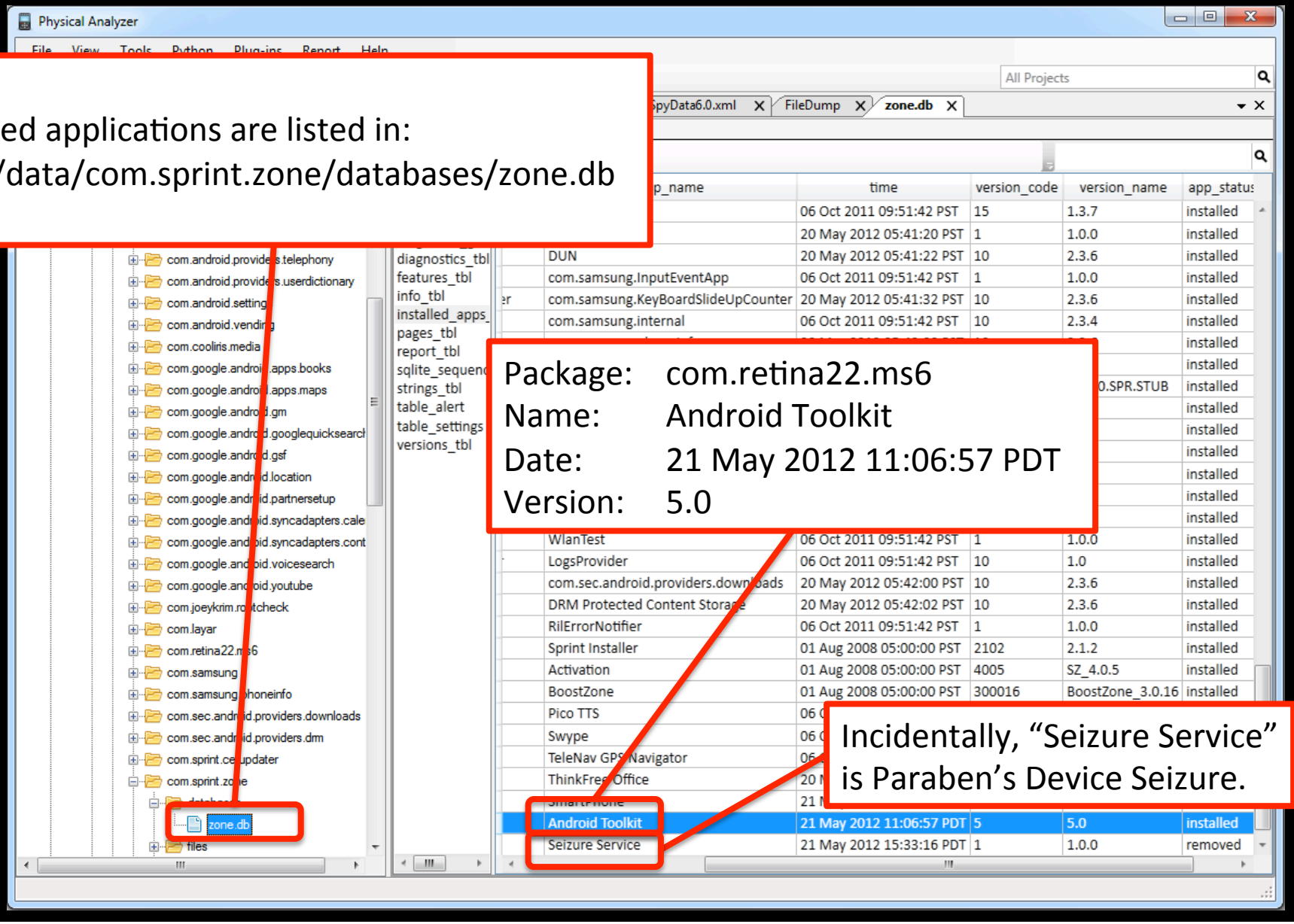
A couple of glitches…

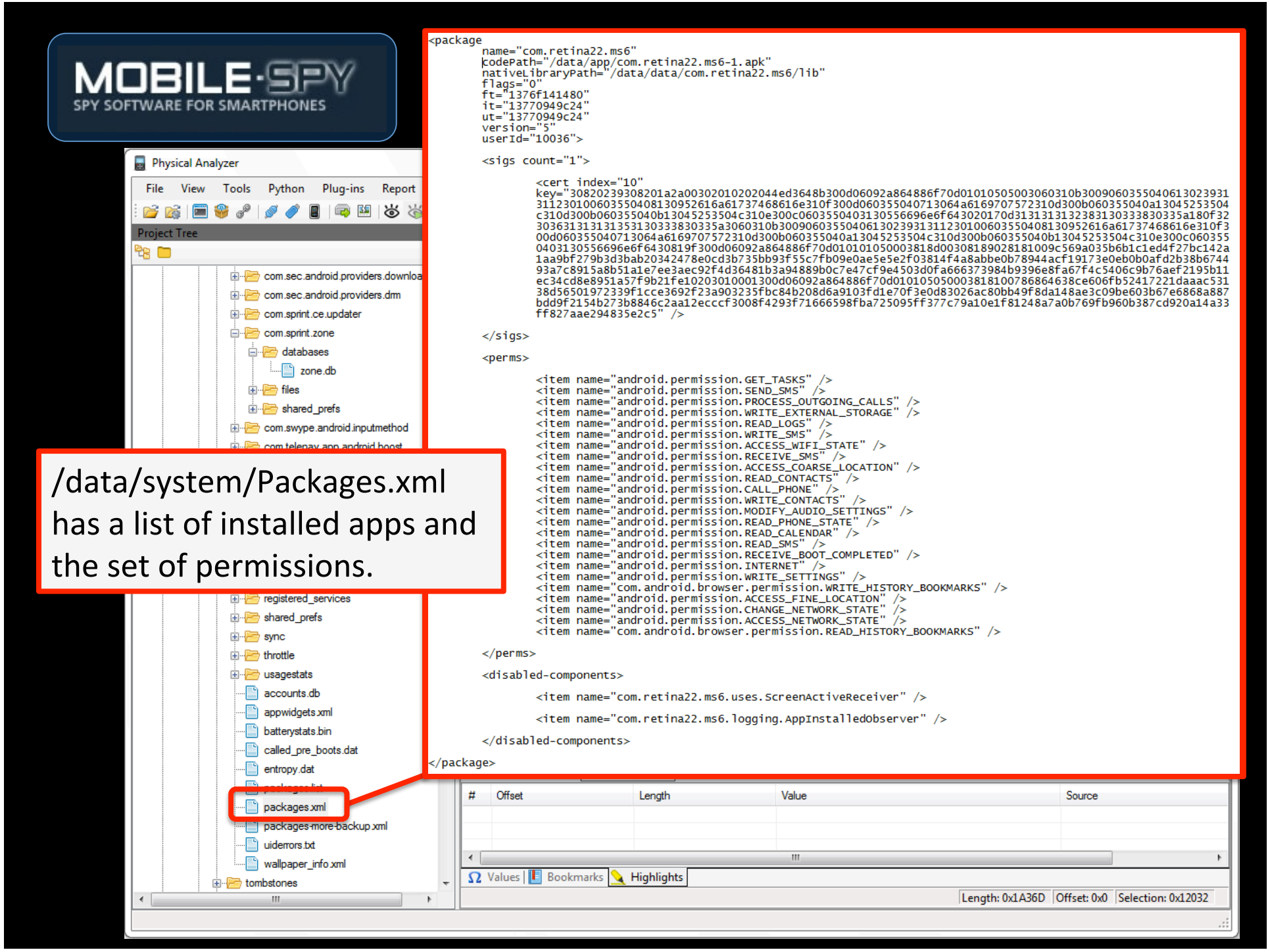
On the version we tested, we noticed:

- E-mail alerts were sent back to a monitoring e-mail address; however, no data appeared on the website.
- After installation, the battery life dropped to 8-10 hours from nearly 20 hours.
- The website requires the user to update his/her password. As a result, the password stored on the device needs to be updated, which means physical access is required again.

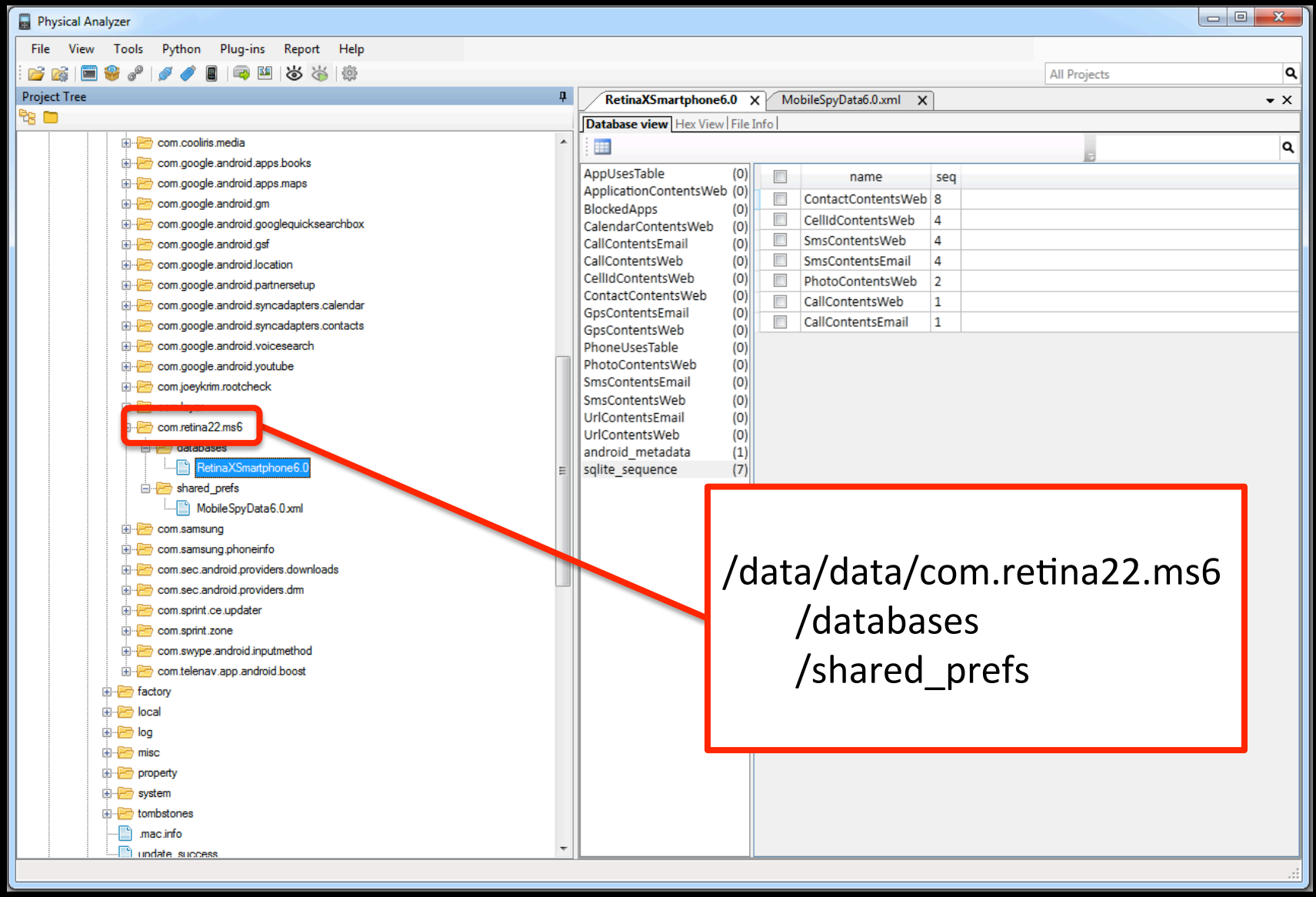
MOBILE·SPY
SPY SOFTWARE FOR SMARTPHONES

Installed applications are listed in:
/data/data/com.sprint.zone/databases/zone.db



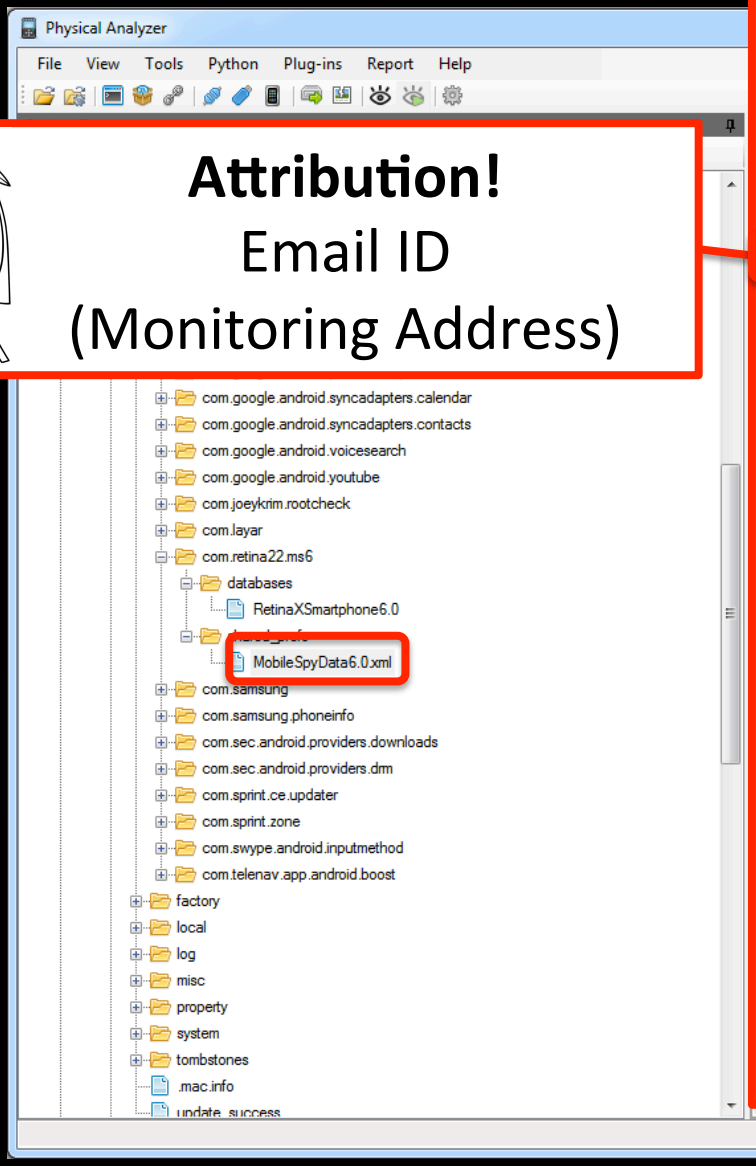

MOBILE·SPY
SPY SOFTWARE FOR SMARTPHONES
Physical Analyzer
File View Tools Python Plug-ins Report
Project Tree
com.sec.android.providers.downloa
com.sec.android.providers.drm
com.sprint.ce.updater
com.sprint.zone
databases
zone.db
files
shared_prefs
com.swype.android.inputmethod
registered_services
shared_prefs
sync
throttle
usagestats
accounts.db
appwidgets.xml
batterystats.bin
called_pre_boots.dat
entropy.dat
packages.xml
packages-more-backup.xml
uiderrors.txt
wallpaper_info.xml
tombstones
/data/system/Packages.xml has a list of installed apps and the set of permissions.
<package
name="com.retina22.ms6"
codePath="/data/app/com.retina22.ms6-1.apk"
nativeLibraryPath="/data/data/com.retina22.ms6/lib"
flags="0"
ft="1376f141480"
it="13770949c24"
ut="13770949c24"
version="5"
userId="10036">
<sigs count="1">
<cert index="10"
key="30820239308201a2a00302010202044ed3648b300d06092a864886f70d01010505003060310b3009060355040613023931
3112301006035504081309526616a61737468616e310f300d0603550407130 64a61697057231 0d300b060355040a13045253504
c310d300b060355040b13045253504c310e300c060355040313055669 6e6f643020170d313131313238313033383035a180f32
303631313131353130333830335a3060310b3009060355040613023931311230100603550408130952616a61737468616e310f3
00d0603550407130 64a61697057231 0d300b060355040a13045253504c310d300b060355040b13045253504c310e300c060355
0403130556696e6f6430819f300d06092a864886f70d01010105000381 8d0030818902818100 9c569a035b6b1c1ed4f27bc142a
1aa9bf279b3d3bab20342478e0cd3b735bb93f55c7fb09e0ae5e5e2f03814f4a8abbe0b78944acf19173e0eb0b0afd2b38b6744
93a7c8915a8b51a1e7ee3aec92f4d36481b3a94889b0c7e47cf9e4503d0fa666373984b9396e8fa67f4c5406c9b76aef2195b11
ec34cd8e8951a57f9b21fe10203010001300d06092a864886f70d01010505000381810078686 4638ce606fb52417221daaac531
38d56501972339f1cce3692f23a903235fbc84b208d6a9103fd1e70f3e0d83026ac80bb49f8da148ae3c09be603b67e6868a887
bdd9f2154b273b8846c2aa12ecccf3008f4293f71666598fba725095ff377c79a10e1f81248a7a0b769fb960b387cd920a14a33
ff827aae294835e2c5" />
</sigs>
<perms>
<item name="android.permission.GET_TASKS" />
<item name="android.permission.SEND_SMS" />
<item name="android.permission.PROCESS_OUTGOING_CALLS" />
<item name="android.permission.WRITE_EXTERNAL_STORAGE" />
<item name="android.permission.READ_LOGS" />
<item name="android.permission.WRITE_SMS" />
<item name="android.permission.ACCESS_WIFI_STATE" />
<item name="android.permission.RECEIVE_SMS" />
<item name="android.permission.ACCESS_COARSE_LOCATION" />
<item name="android.permission.READ_CONTACTS" />
<item name="android.permission.CALL_PHONE" />
<item name="android.permission.WRITE_CONTACTS" />
<item name="android.permission.MODIFY_AUDIO_SETTINGS" />
<item name="android.permission.READ_PHONE_STATE" />
<item name="android.permission.READ_CALENDAR" />
<item name="android.permission.READ_SMS" />
<item name="android.permission.RECEIVE_BOOT_COMPLETED" />
<item name="android.permission.INTERNET" />
<item name="android.permission.WRITE_SETTINGS" />
<item name="com.android.browser.permission.WRITE_HISTORY_BOOKMARKS" />
<item name="android.permission.ACCESS_FINE_LOCATION" />
<item name="android.permission.CHANGE_NETWORK_STATE" />
<item name="android.permission.ACCESS_NETWORK_STATE" />
<item name="com.android.browser.permission.READ_HISTORY_BOOKMARKS" />
</perms>
<disabled-components>
<item name="com.retina22.ms6.uses.ScreenActiveReceiver" />
<item name="com.retina22.ms6.logging.AppInstalledObserver" />
</disabled-components>
</package>
Offset Length Value Source
Values Bookmarks Highlights
Length: 0x1A36D Offset: 0x0 Selection: 0x12032

MOBILE·SPY
SPY SOFTWARE FOR SMARTPHONES



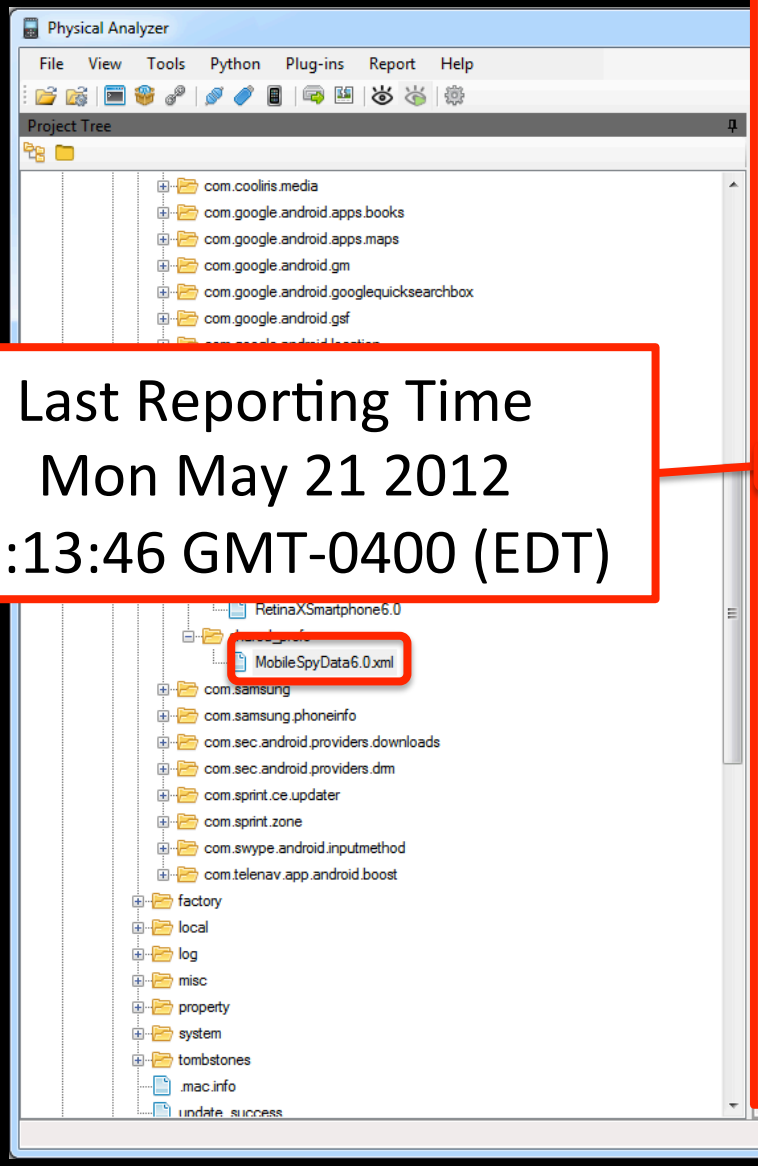
MOBILE·SPY
SPY SOFTWARE FOR SMARTPHONES

Attribution!
Email ID
(Monitoring Address)




```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="KEY_IS_GPS_INFO_CMD" value="true" />
<boolean name="KEY_CELLID_LOG" value="true" />
<int name="KEY_GPS_INTERVAL" value="15" />
<string name="KEY_USER_NAME">Prevail</string>
<long name="KEY_SMS_ID" value="12" />
<long name="KEY_PICTURE_ID" value="2" />
<boolean name="KEY_IS_EMAIL_GPS" value="true" />
<string name="KEY_EMAIL_ID">[redacted]@gmail.com</string>
<boolean name="KEY_IS_SIM_CHANGE_NOTIFICATION" value="true" />
<boolean name="KEY_IS_EMAIL_ALERT" value="true" />
<boolean name="KEY_IS_EMAIL_REPORT" value="true" />
<int name="KEY_XML_UPLOADER_TIME" value="30" />
<boolean name="KEY_LOCK_LOG" value="true" />
<long name="KEY_LAST_REPORTING_TIME" value="1337649226670" />
<boolean name="KEY_IS_SIM_INFO_CMD" value="true" />
<string name="KEY_IMSI_NUMBER">310[redacted]</string>
<boolean name="KEY_IS_EMAIL_SMS" value="true" />
<boolean name="KEY_IS_ACTIVE" value="true" />
<boolean name="KEY_WIPE_LOG" value="true" />
<long name="KEY_CONTACT_ID" value="8" />
<int name="KEY_ACCOUNT_PULLER_TIME" value="345" />
<boolean name="KEY_IS_EMAIL_CALL" value="true" />
<boolean name="KEY_GPS_LOG" value="false" />
<string name="KEY_FRIEND_NUM">410[redacted]</string>
<boolean name="KEY_IS_EMAIL_URL" value="true" />
<long name="KEY_CALL_ID" value="7" />
<boolean name="KEY_IS_FIRST_TIME" value="false" />
<int name="KEY_EMAIL_INTERVAL" value="15" />
<string name="KEY_USER_ID">1000[redacted]</string>
<boolean name="KEY_IS_LIVE_PANEL" value="true" />
</map>
```

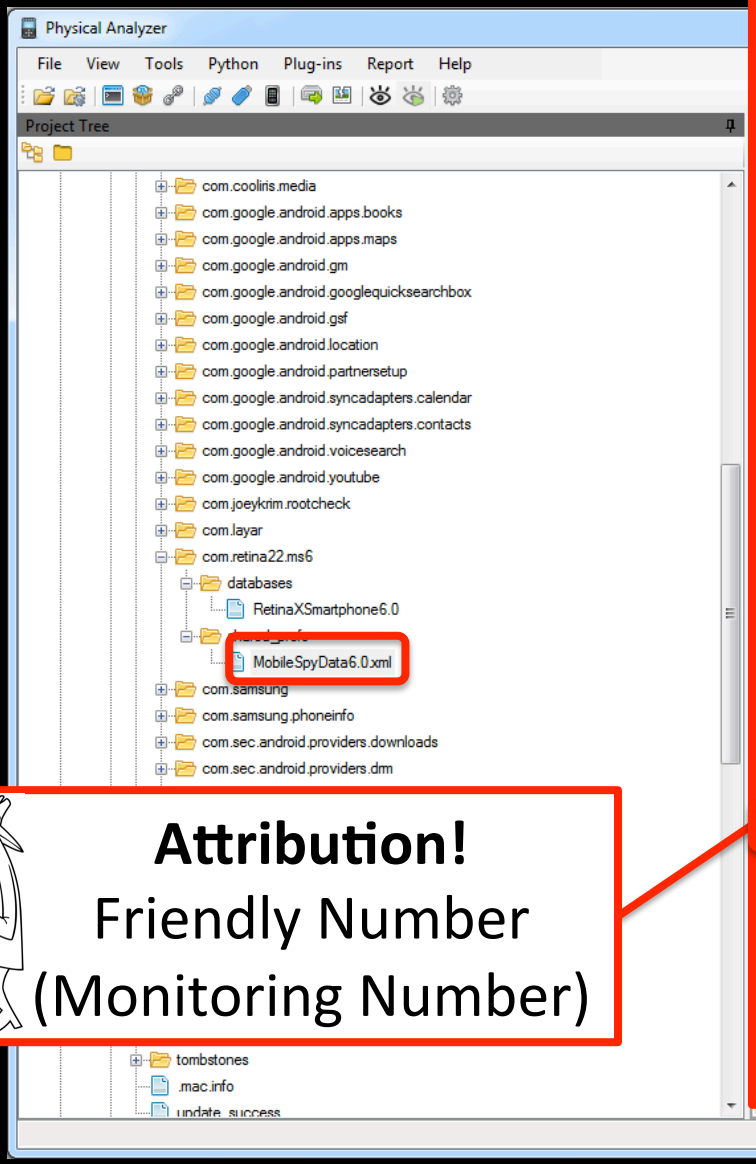
MOBILE·SPY
SPY SOFTWARE FOR SMARTPHONES



Last Reporting Time
Mon May 21 2012
21:13:46 GMT-0400 (EDT)

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="KEY_IS_GPS_INFO_CMD" value="true" />
<boolean name="KEY_CELLID_LOG" value="true" />
<int name="KEY_GPS_INTERVAL" value="15" />
<string name="KEY_USER_NAME">Prevail</string>
<long name="KEY_SMS_ID" value="12" />
<long name="KEY_PICTURE_ID" value="2" />
<boolean name="KEY_IS_EMAIL_GPS" value="true" />
<string name="KEY_EMAIL_ID">[redacted]@gmail.com</string>
<boolean name="KEY_IS_SIM_CHANGE_NOTIFICATION" value="true" />
<boolean name="KEY_IS_EMAIL_ALERT" value="true" />
<boolean name="KEY_IS_EMAIL_REPORT" value="true" />
<int name="KEY_XML_UPLOADER_TIME" value="30" />
<boolean name="KEY_LOCK_LOG" value="true" />
<long name="KEY_LAST_REPORTING_TIME" value="1337649226670" />
<boolean name="KEY_IS_SIM_INFO_CMD" value="true" />
<string name="KEY_IMSI_NUMBER">310[redacted]</string>
<boolean name="KEY_IS_EMAIL_SMS" value="true" />
<boolean name="KEY_IS_ACTIVE" value="true" />
<boolean name="KEY_WIPE_LOG" value="true" />
<long name="KEY_CONTACT_ID" value="8" />
<int name="KEY_ACCOUNT_PULLER_TIME" value="345" />
<boolean name="KEY_IS_EMAIL_CALL" value="true" />
<boolean name="KEY_GPS_LOG" value="false" />
<string name="KEY_FRIEND_NUM">410[redacted]</string>
<boolean name="KEY_IS_EMAIL_URL" value="true" />
<long name="KEY_CALL_ID" value="7" />
<boolean name="KEY_IS_FIRST_TIME" value="false" />
<int name="KEY_EMAIL_INTERVAL" value="15" />
<string name="KEY_USER_ID">1000[redacted]</string>
<boolean name="KEY_IS_LIVE_PANEL" value="true" />
</map>
```

MOBILE·SPY
SPY SOFTWARE FOR SMARTPHONES

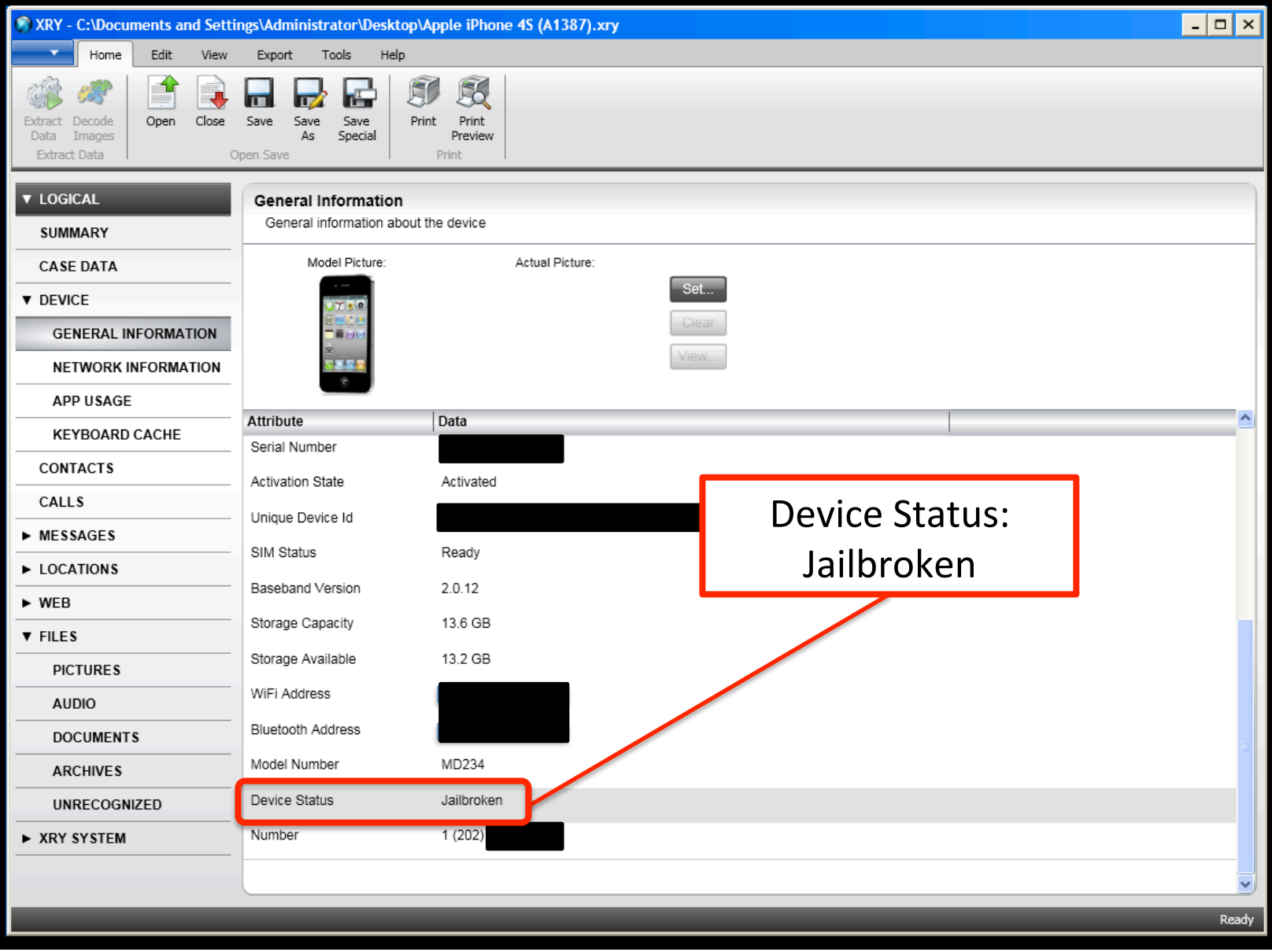


Attribution!
Friendly Number
(Monitoring Number)

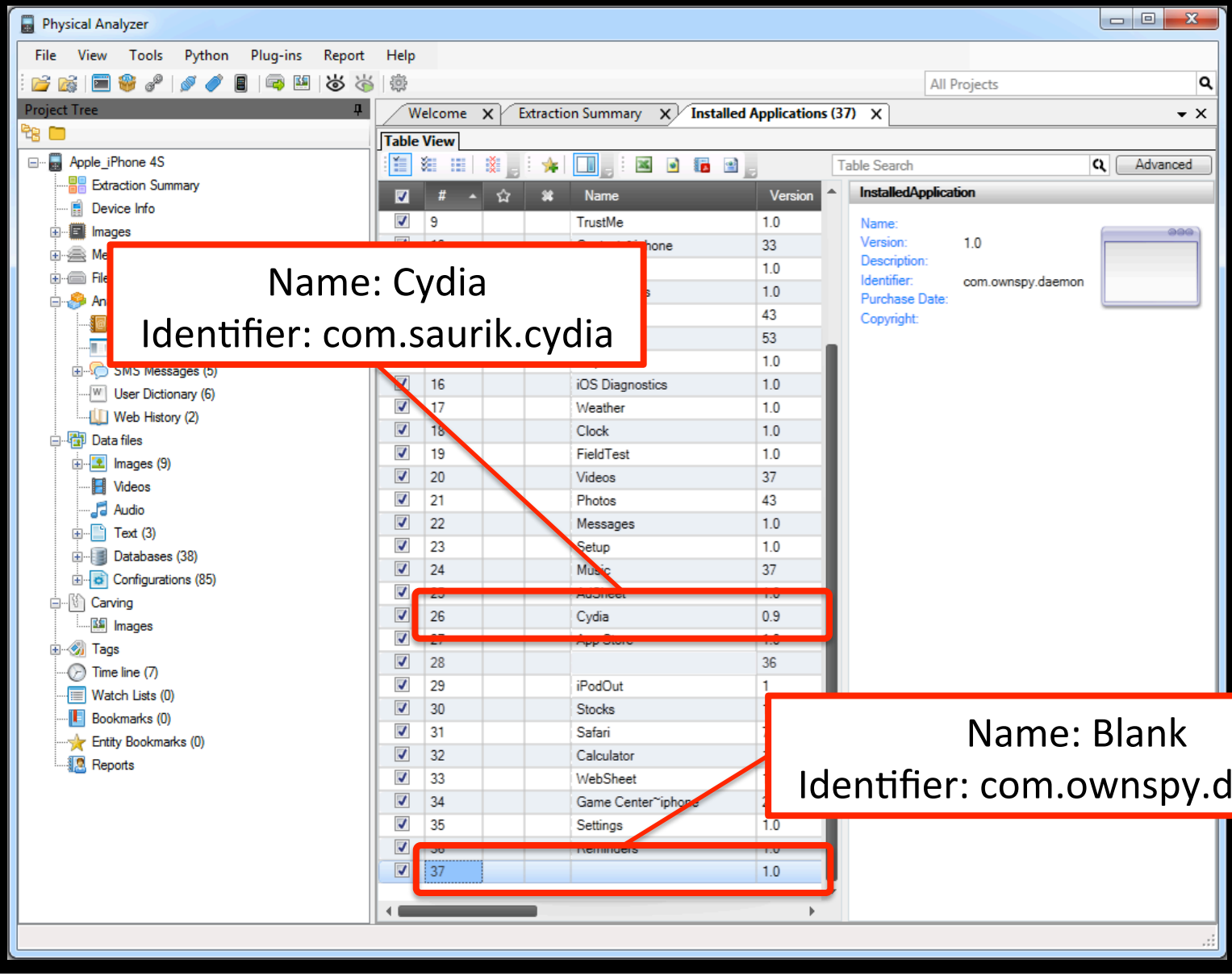
```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="KEY_IS_GPS_INFO_CMD" value="true" />
<boolean name="KEY_CELLID_LOG" value="true" />
<int name="KEY_GPS_INTERVAL" value="15" />
<string name="KEY_USER_NAME">Prevail</string>
<long name="KEY_SMS_ID" value="12" />
<long name="KEY_PICTURE_ID" value="2" />
<boolean name="KEY_IS_EMAIL_GPS" value="true" />
<string name="KEY_EMAIL_ID">[redacted]@gmail.com</string>
<boolean name="KEY_IS_SIM_CHANGE_NOTIFICATION" value="true" />
<boolean name="KEY_IS_EMAIL_ALERT" value="true" />
<boolean name="KEY_IS_EMAIL_REPORT" value="true" />
<int name="KEY_XML_UPLOADER_TIME" value="30" />
<boolean name="KEY_LOCK_LOG" value="true" />
<long name="KEY_LAST_REPORTING_TIME" value="1337649226670" />
<boolean name="KEY_IS_SIM_INFO_CMD" value="true" />
<string name="KEY_IMSI_NUMBER">31[redacted]</string>
<boolean name="KEY_IS_EMAIL_SMS" value="true" />
<boolean name="KEY_IS_ACTIVE" value="true" />
<boolean name="KEY_WIPE_LOG" value="true" />
<long name="KEY_CONTACT_ID" value="8" />
<int name="KEY_ACCOUNT_PULLER_TIME" value="345" />
<boolean name="KEY_IS_EMAIL_CALL" value="true" />
<boolean name="KEY_GPS_LOG" value="false" />
<string name="KEY_FRIEND_NUM">410[redacted]</string>
<boolean name="KEY_IS_EMAIL_URL" value="true" />
<long name="KEY_CALL_ID" value="7" />
<boolean name="KEY_IS_FIRST_TIME" value="false" />
<int name="KEY_EMAIL_INTERVAL" value="15" />
<string name="KEY_USER_ID">1000[redacted]</string>
<boolean name="KEY_IS_LIVE_PANEL" value="true" />
</map>
```

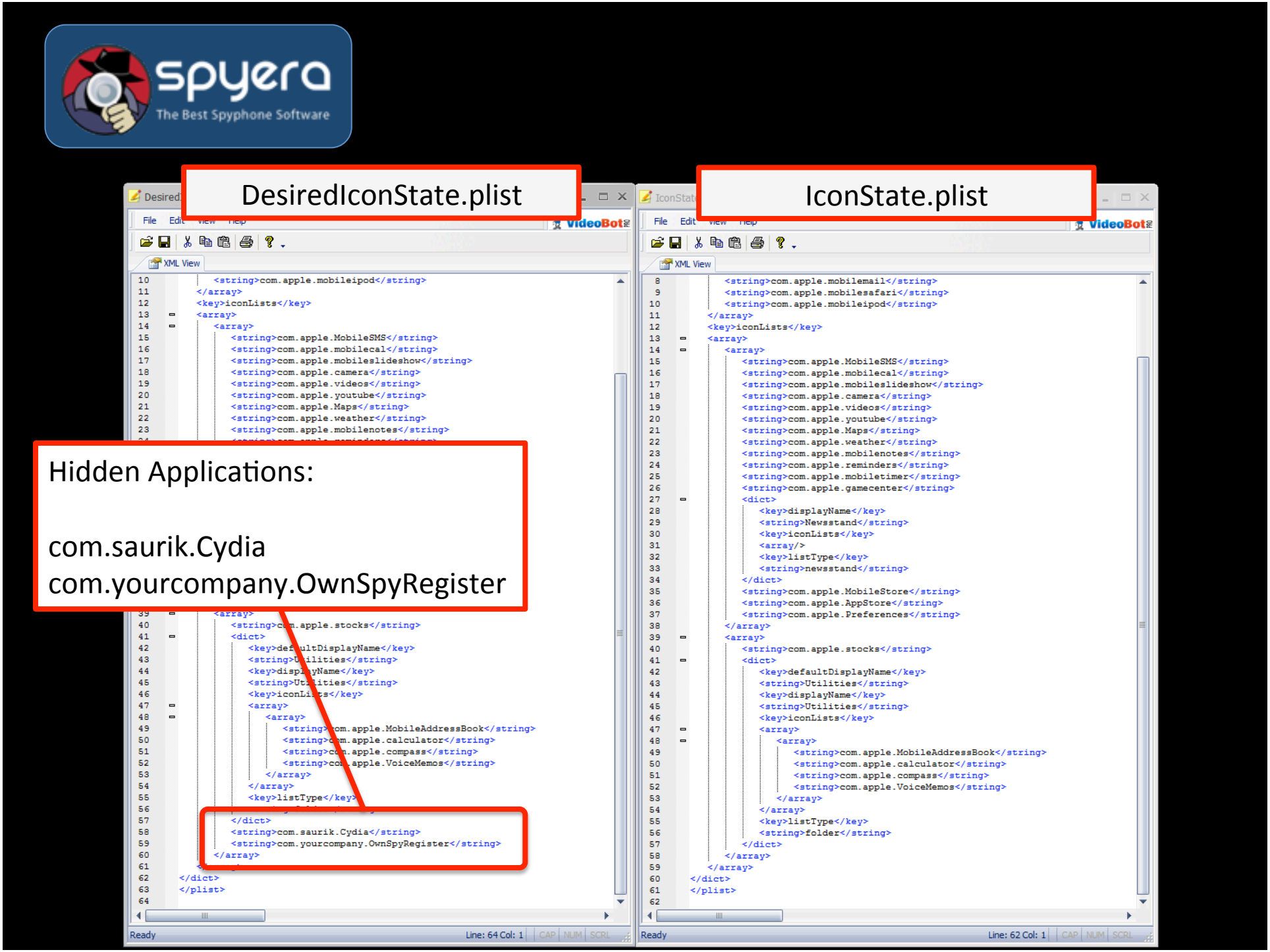

spyera
The Best Spyphone Software

Evidence of Jailbreaking

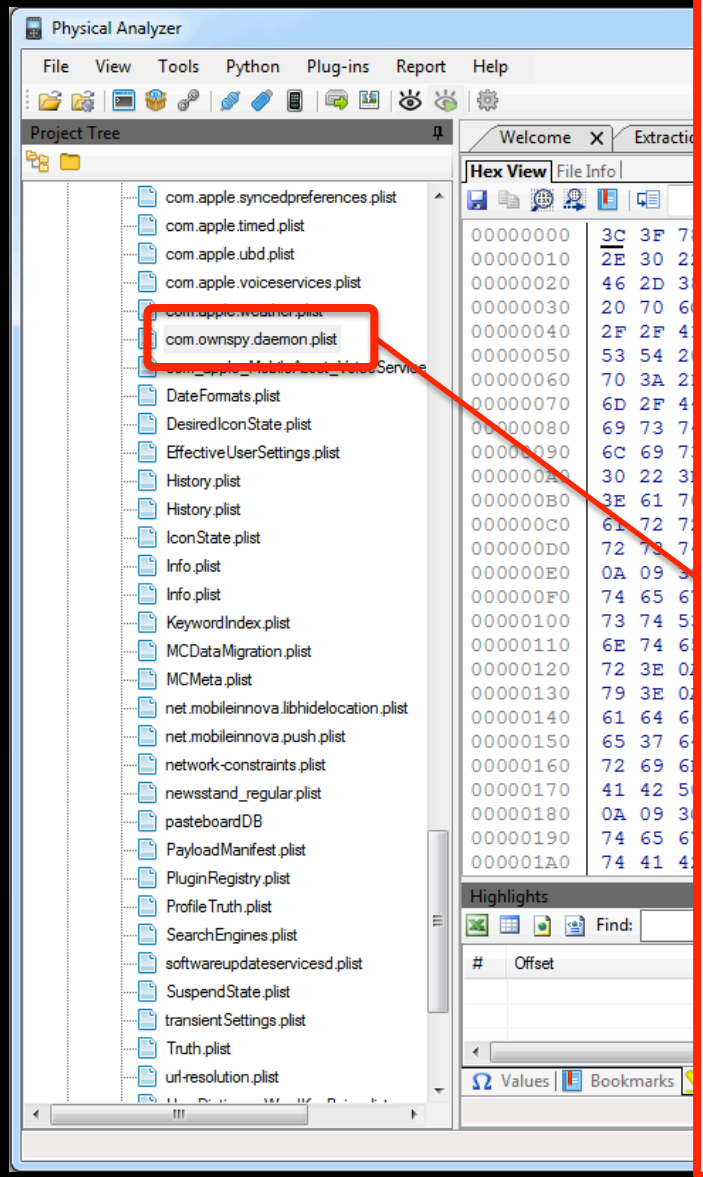


Installed Applications




spyera
The Best Spyphone Software
DesiredIconState.plist
IconState.plist
Hidden Applications:
com.saurik.Cydia
com.yourcompany.OwnSpyRegister

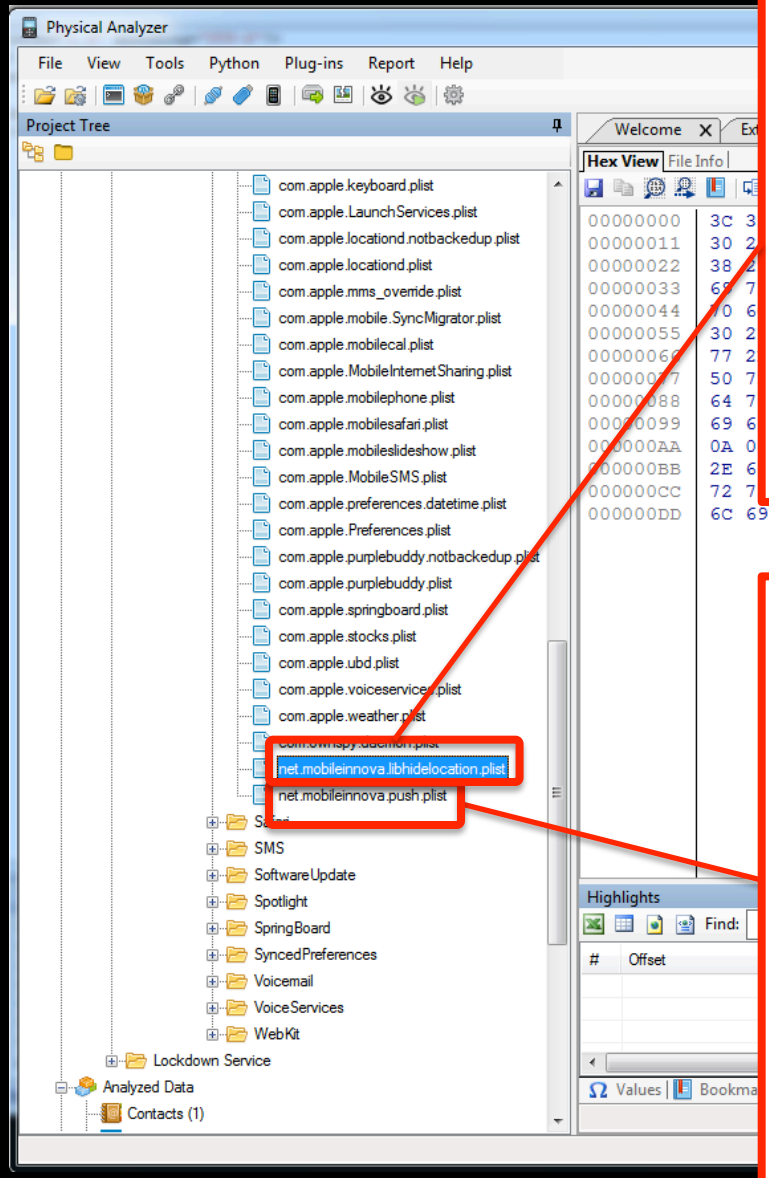
/data/data/com.radioadv/shared_prefs/




```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0”>
<dict>
<key>applog</key>
<array/>
<key>firstPicture</key>
<integer>1</integer>
<key>firstSync</key>
<integer>1</integer>
<key>key</key>
<string>[redacted]</string>
<key>lastABPersonID</key>
<integer>2</integer>
<key>lastABValueID</key>
<integer>1</integer>
<key>lastCHread</key>
<integer>1</integer>
<key>lastSMSread</key>
<integer>5</integer>
<key>lastWHDate</key>
<real>360668832</real>
</dict>
</plist>
```

Attribution!
Unique Key

/var/mobile/Library/preferences/

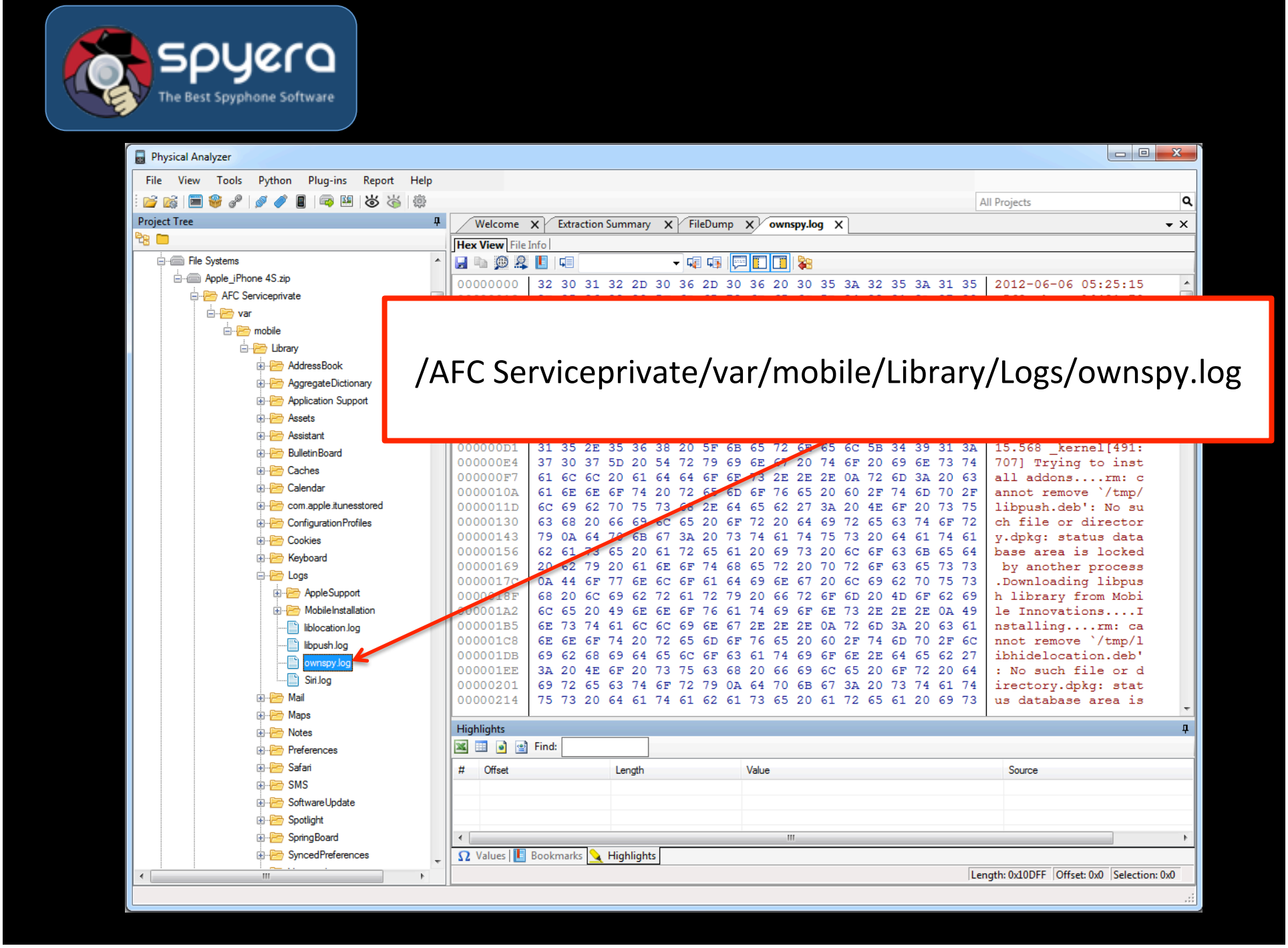


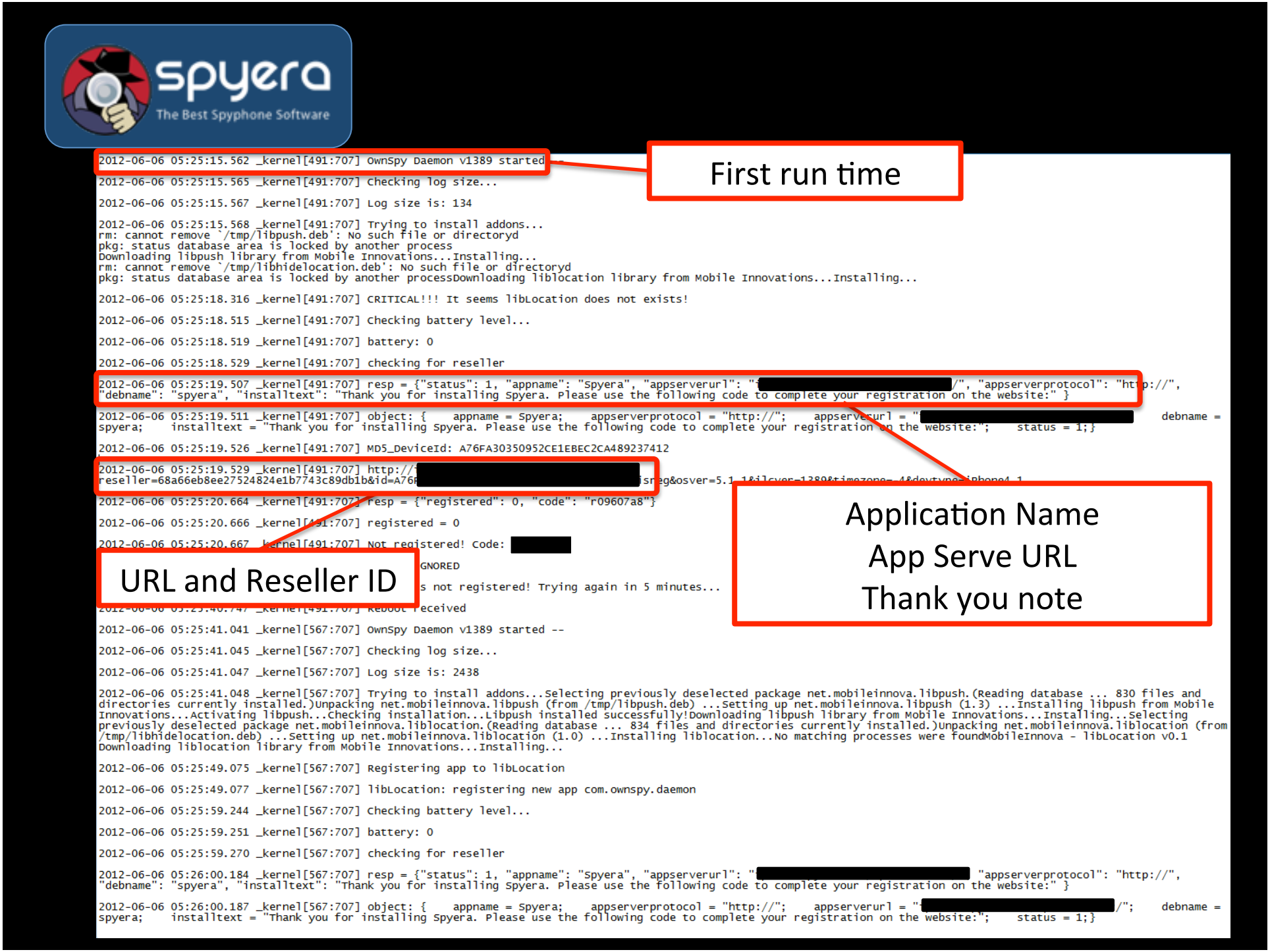
net.mobileinnova.libhidelocation.plist

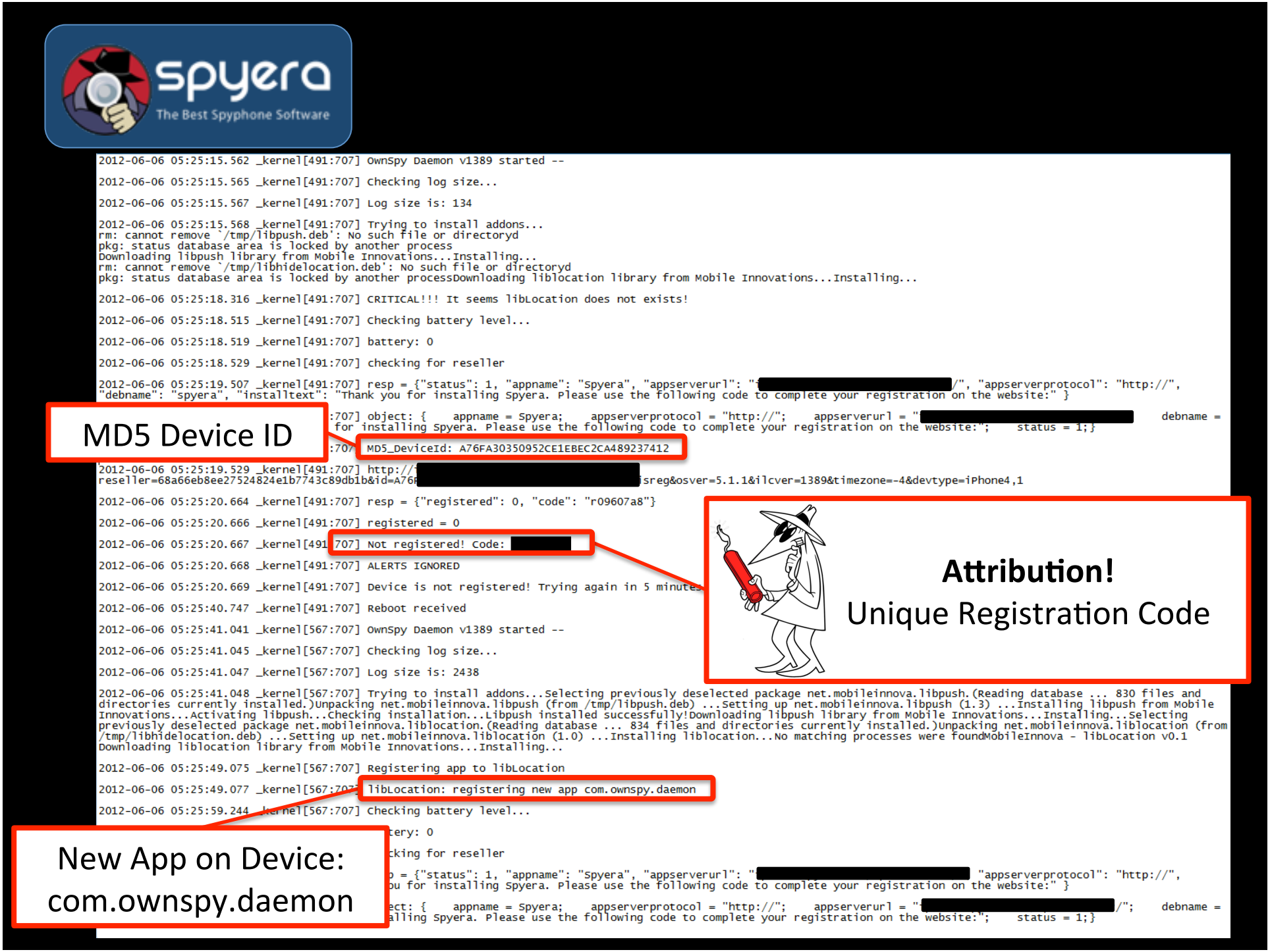
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
http://www.apple.com/DTDs/PropertyList-1.0.dtd>
<plist version="1.0”>
<dict>
<key>com.ownspy.daemon</key>
<true/>
</dict>
</plist>
```

net.mobileinnova.push.plist

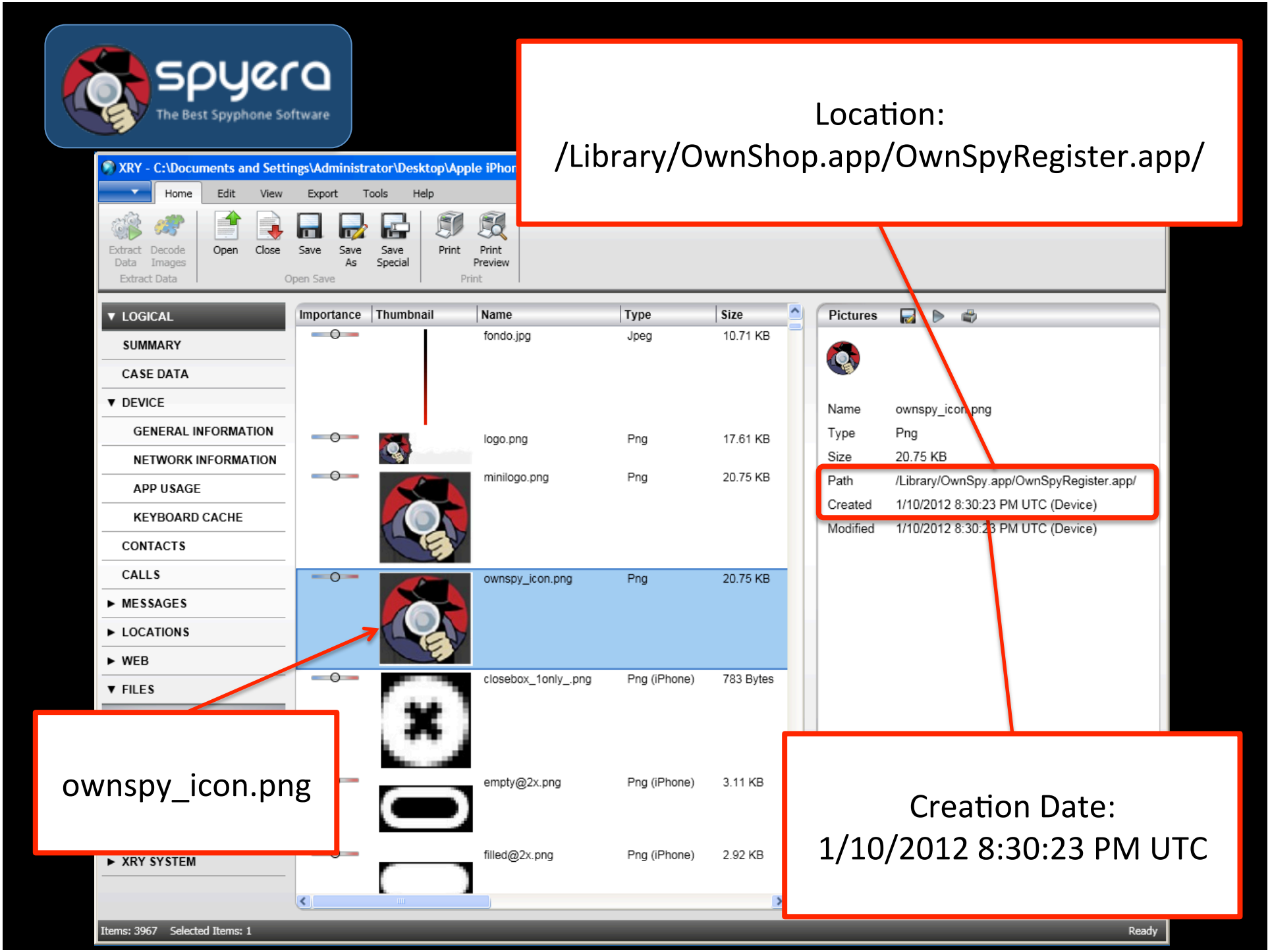
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
http://www.apple.com/DTDs/PropertyList-1.0.dtd>
<plist version="1.0”>
<dict>
<key>services</key>
<array>
<string>com.ownspy.daemon</string>
</array>
</dict>
</plist>
```

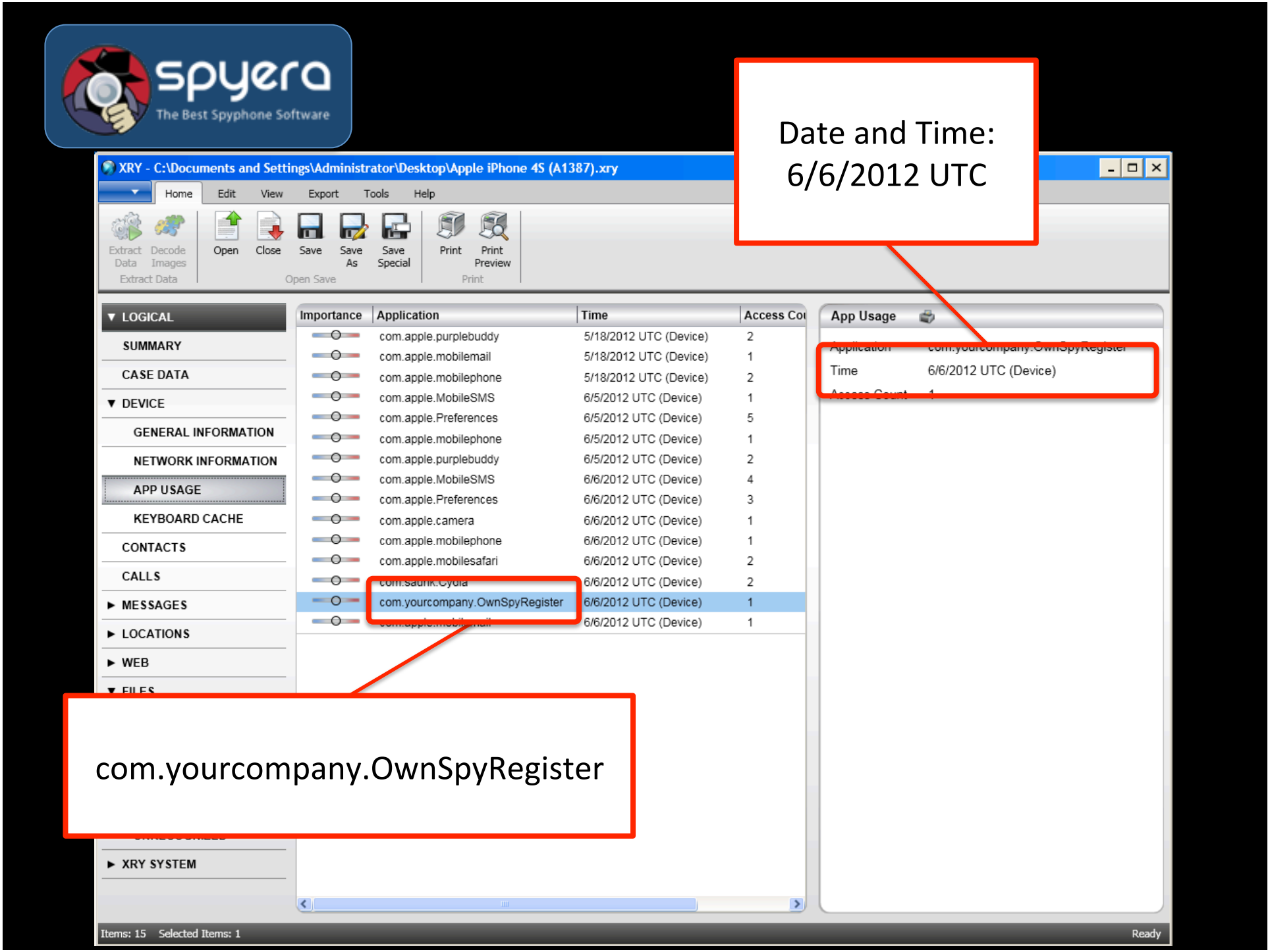

spyera
The Best Spyphone Software
Physical Analyzer
File View Tools Python Plug-ins Report Help
All Projects
Project Tree
Welcome
Extraction Summary
FileDump
ownspy.log
Hex View
File Info
00000000 32 30 31 32 2D 30 36 2D 30 36 20 30 35 3A 32 35 3A 31 35 2012-06-06 05:25:15
/AFC Serviceprivate/var/mobile/Library/Logs/ownspy.log
File Systems
Apple_iPhone 4S.zip
AFC Serviceprivate
var
mobile
Library
AddressBook
AggregateDictionary
Application Support
Assets
Assistant
BulletinBoard
Caches
Calendar
com.apple.itunesstored
ConfigurationProfiles
Cookies
Keyboard
Logs
AppleSupport
MobileInstallation
liblocation.log
libpush.log
ownspy.log
Siri.log
Mail
Maps
Notes
Preferences
Safari
SMS
SoftwareUpdate
Spotlight
SpringBoard
SyncedPreferences
000000D1 31 35 2E 35 36 38 20 5F 6B 65 72 6E 65 6C 5B 34 39 31 3A 15.568 _kernel[491:
000000E4 37 30 37 5D 20 54 72 79 69 6E 67 20 74 6F 20 69 6E 73 74 707] Trying to inst
000000F7 61 6C 6C 20 61 64 64 6F 6E 73 2E 2E 2E 0A 72 6D 3A 20 63 all addons....rm: c
0000010A 61 6E 6E 6F 74 20 72 65 6D 6F 76 65 20 60 2F 74 6D 70 2F annot remove `/tmp/
0000011D 6C 69 62 70 75 73 68 2E 64 65 62 27 3A 20 4E 6F 20 73 75 libpush.deb': No su
00000130 63 68 20 66 69 6C 65 20 6F 72 20 64 69 72 65 63 74 6F 72 ch file or director
00000143 79 0A 64 70 6B 67 3A 20 73 74 61 74 75 73 20 64 61 74 61 y.dpkg: status data
00000156 62 61 73 65 20 61 72 65 61 20 69 73 20 6C 6F 63 6B 65 64 base area is locked
00000169 20 62 79 20 61 6E 6F 74 68 65 72 20 70 72 6F 63 65 73 73 by another process
0000017C 0A 44 6F 77 6E 6C 6F 61 64 69 6E 67 20 6C 69 62 70 75 73 .Downloading libpus
0000018F 68 20 6C 69 62 72 61 72 79 20 66 72 6F 6D 20 4D 6F 62 69 h library from Mobi
000001A2 6C 65 20 49 6E 6E 6F 76 61 74 69 6F 6E 73 2E 2E 2E 0A 49 le Innovations....I
000001B5 6E 73 74 61 6C 6C 69 6E 67 2E 2E 2E 0A 72 6D 3A 20 63 61 nstalling....rm: ca
000001C8 6E 6E 6F 74 20 72 65 6D 6F 76 65 20 60 2F 74 6D 70 2F 6C nnot remove `/tmp/l
000001DB 69 62 68 69 64 65 6C 6F 63 61 74 69 6F 6E 2E 64 65 62 27 ibhidelocation.deb'
000001EE 3A 20 4E 6F 20 73 75 63 68 20 66 69 6C 65 20 6F 72 20 64 : No such file or d
00000201 69 72 65 63 74 6F 72 79 0A 64 70 6B 67 3A 20 73 74 61 74 irectory.dpkg: stat
00000214 75 73 20 64 61 74 61 62 61 73 65 20 61 72 65 61 20 69 73 us database area is
Highlights
Find:
Offset Length Value Source
Values Bookmarks Highlights
Length: 0x10DFF Offset: 0x0 Selection: 0x0

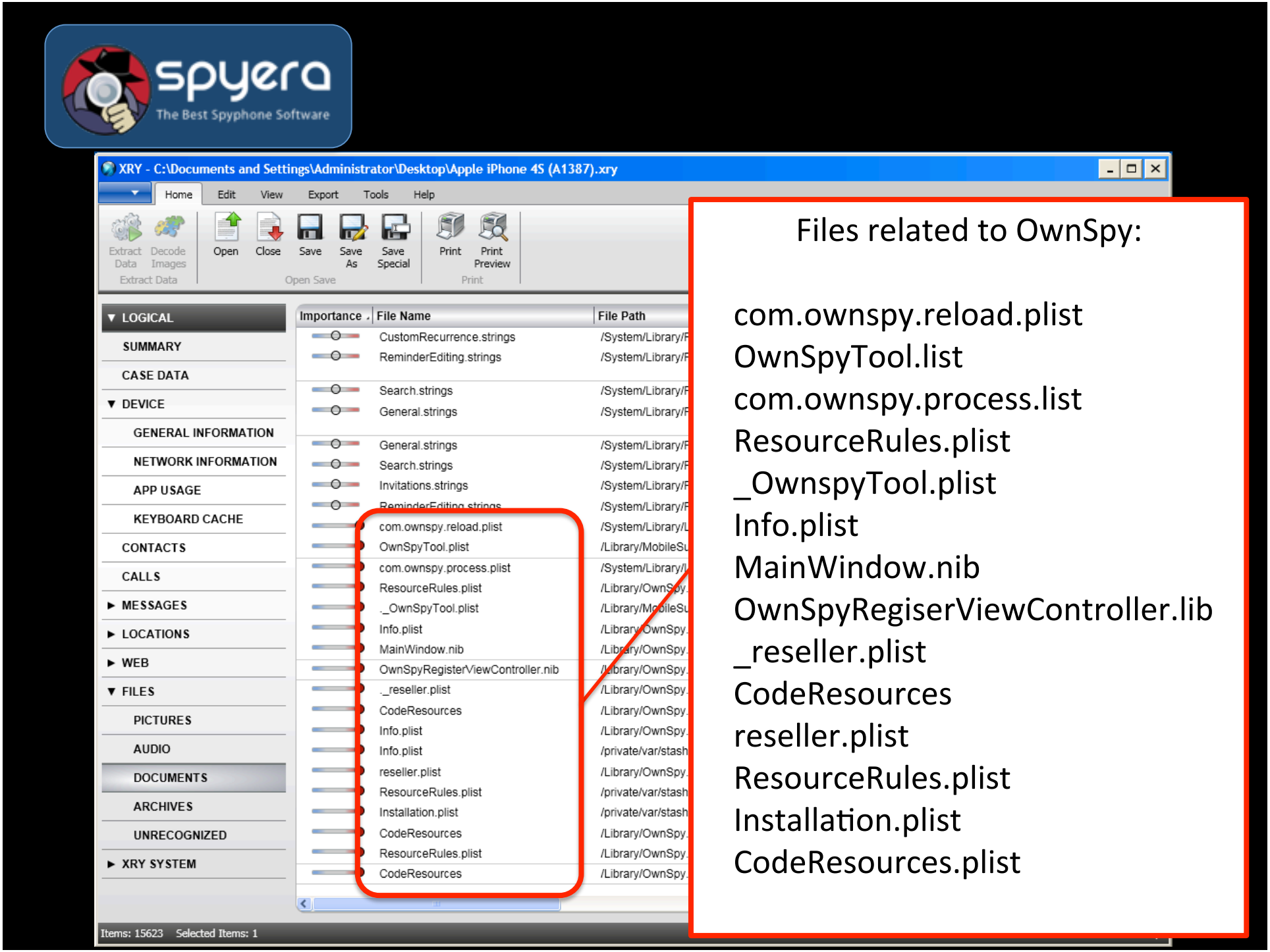

spyera
The Best Spyphone Software
2012-06-06 05:25:15.562 _kernel[491:707] OwnSpy Daemon v1389 started --
First run time
2012-06-06 05:25:15.565 _kernel[491:707] Checking log size...
2012-06-06 05:25:15.567 _kernel[491:707] Log size is: 134
2012-06-06 05:25:15.568 _kernel[491:707] Trying to install addons...
rm: cannot remove `/tmp/libpush.deb': No such file or directoryd
pkg: status database area is locked by another process
Downloading libpush library from Mobile Innovations...Installing...
rm: cannot remove `/tmp/libhidelocation.deb': No such file or directoryd
pkg: status database area is locked by another processDownloading liblocation library from Mobile Innovations...Installing...
2012-06-06 05:25:18.316 _kernel[491:707] CRITICAL!!! It seems libLocation does not exists!
2012-06-06 05:25:18.515 _kernel[491:707] Checking battery level...
2012-06-06 05:25:18.519 _kernel[491:707] battery: 0
2012-06-06 05:25:18.529 _kernel[491:707] checking for reseller
2012-06-06 05:25:19.507 _kernel[491:707] resp = {"status": 1, "appname": "Spyera", "appserverurl": "
"debname": "spyera", "installtext": "Thank you for installing Spyera. Please use the following code to complete your registration on the website:" }
2012-06-06 05:25:19.511 _kernel[491:707] object: { appname = Spyera; appserverprotocol = "http://"; appserverurl = "
spyera; installtext = "Thank you for installing Spyera. Please use the following code to complete your registration on the website:"; status = 1;}
2012-06-06 05:25:19.526 _kernel[491:707] MD5_DeviceId: A76FA30350952CE1EBEC2CA489237412
2012-06-06 05:25:19.529 _kernel[491:707] http://
reseller=68a66eb8ee27524824e1b7743c89db1b&id=A76
URL and Reseller ID
2012-06-06 05:25:20.664 _kernel[491:707] resp = {"registered": 0, "code": "r09607a8"}
2012-06-06 05:25:20.666 _kernel[491:707] registered = 0
2012-06-06 05:25:20.667 _kernel[491:707] Not registered! Code:
GNORED
s not registered! Trying again in 5 minutes...
Application Name
App Serve URL
Thank you note
2012-06-06 05:25:41.041 _kernel[567:707] OwnSpy Daemon v1389 started --
2012-06-06 05:25:41.045 _kernel[567:707] Checking log size...
2012-06-06 05:25:41.047 _kernel[567:707] Log size is: 2438
2012-06-06 05:25:41.048 _kernel[567:707] Trying to install addons...Selecting previously deselected package net.mobileinnova.libpush.(Reading database ... 830 files and directories currently installed.)Unpacking net.mobileinnova.libpush (from /tmp/libpush.deb) ...Setting up net.mobileinnova.libpush (1.3) ...Installing libpush from Mobile Innovations...Activating libpush...Checking installation...Libpush installed successfully!Downloading libpush library from Mobile Innovations...Installing...Selecting previously deselected package net.mobileinnova.liblocation.(Reading database ... 834 files and directories currently installed.)Unpacking net.mobileinnova.liblocation (from /tmp/libhidelocation.deb) ...Setting up net.mobileinnova.liblocation (1.0) ...Installing liblocation...No matching processes were foundMobileInnova - libLocation v0.1
Downloading liblocation library from Mobile Innovations...Installing...
2012-06-06 05:25:49.075 _kernel[567:707] Registering app to libLocation
2012-06-06 05:25:49.077 _kernel[567:707] libLocation: registering new app com.ownspy.daemon
2012-06-06 05:25:59.244 _kernel[567:707] Checking battery level...
2012-06-06 05:25:59.251 _kernel[567:707] battery: 0
2012-06-06 05:25:59.270 _kernel[567:707] checking for reseller
2012-06-06 05:26:00.184 _kernel[567:707] resp = {"status": 1, "appname": "Spyera", "appserverurl": "
"debname": "spyera", "installtext": "Thank you for installing Spyera. Please use the following code to complete your registration on the website:" }
2012-06-06 05:26:00.187 _kernel[567:707] object: { appname = Spyera; appserverprotocol = "http://"; appserverurl = "
spyera; installtext = "Thank you for installing Spyera. Please use the following code to complete your registration on the website:"; status = 1;}

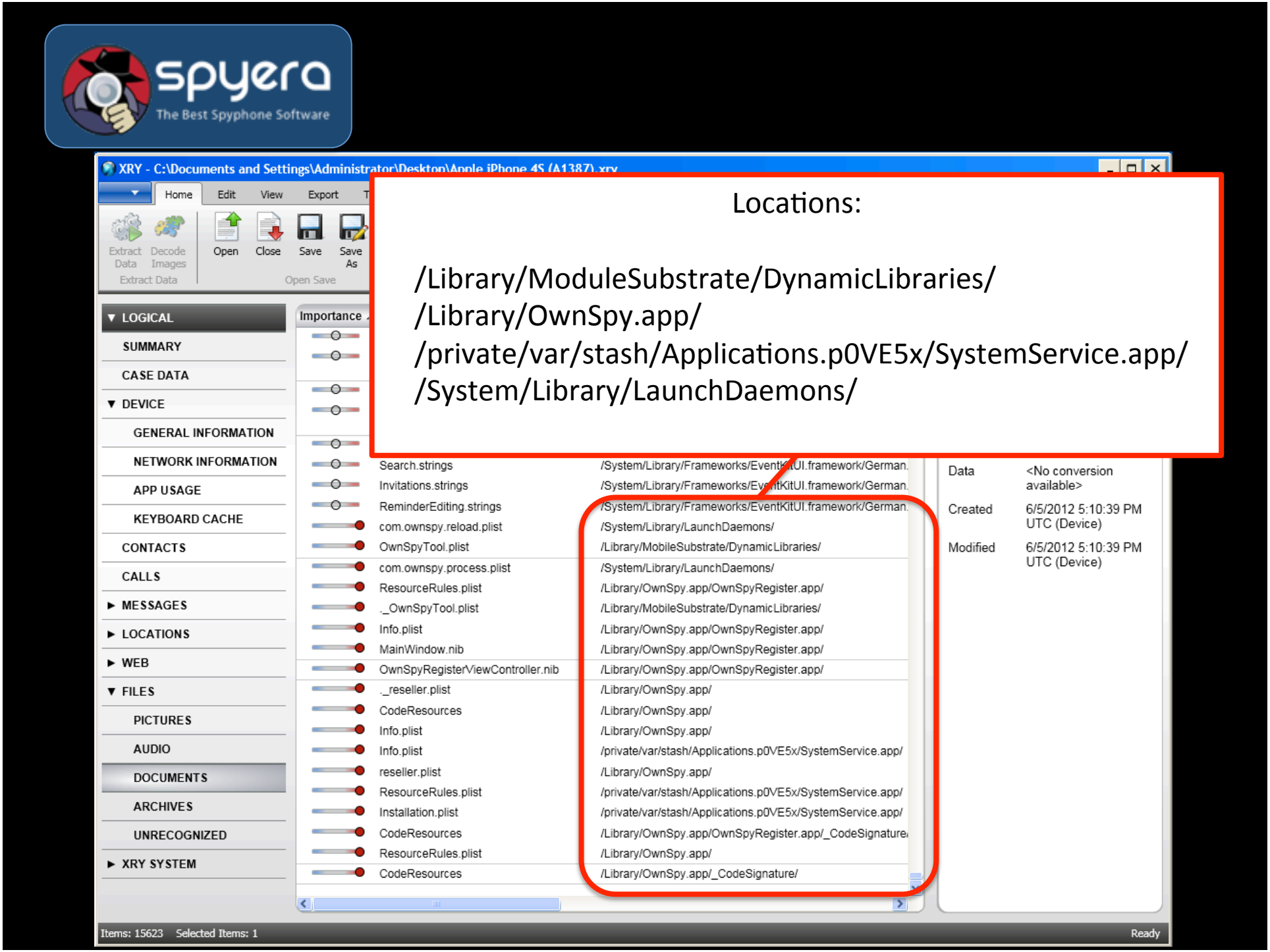

spyera
The Best Spyphone Software
2012-06-06 05:25:15.562 _kernel[491:707] OwnSpy Daemon v1389 started --
2012-06-06 05:25:15.565 _kernel[491:707] Checking log size...
2012-06-06 05:25:15.567 _kernel[491:707] Log size is: 134
2012-06-06 05:25:15.568 _kernel[491:707] Trying to install addons...
rm: cannot remove `/tmp/libpush.deb': No such file or directoryd
pkg: status database area is locked by another process
Downloading libpush library from Mobile Innovations...Installing...
rm: cannot remove `/tmp/libhidelocation.deb': No such file or directoryd
pkg: status database area is locked by another processDownloading liblocation library from Mobile Innovations...Installing...
2012-06-06 05:25:18.316 _kernel[491:707] CRITICAL!!! It seems libLocation does not exists!
2012-06-06 05:25:18.515 _kernel[491:707] Checking battery level...
2012-06-06 05:25:18.519 _kernel[491:707] battery: 0
2012-06-06 05:25:18.529 _kernel[491:707] checking for reseller
2012-06-06 05:25:19.507 _kernel[491:707] resp = {"status": 1, "appname": "Spyera", "appserverurl": "
"debname": "spyera", "installtext": "Thank you for installing Spyera. Please use the following code to complete your registration on the website:" }
MD5 Device ID
MD5_DeviceId: A76FA30350952CE1EBEC2CA489237412
2012-06-06 05:25:19.529 _kernel[491:707] http://
reseller=68a66eb8ee27524824e1b7743c89db1b&id=A76
2012-06-06 05:25:20.664 _kernel[491:707] resp = {"registered": 0, "code": "r09607a8"}
2012-06-06 05:25:20.666 _kernel[491:707] registered = 0
2012-06-06 05:25:20.667 _kernel[491:707] Not registered! Code:
2012-06-06 05:25:20.668 _kernel[491:707] ALERTS IGNORED
2012-06-06 05:25:20.669 _kernel[491:707] Device is not registered! Trying again in 5 minutes
2012-06-06 05:25:40.747 _kernel[491:707] Reboot received
2012-06-06 05:25:41.041 _kernel[567:707] OwnSpy Daemon v1389 started --
2012-06-06 05:25:41.045 _kernel[567:707] Checking log size...
2012-06-06 05:25:41.047 _kernel[567:707] Log size is: 2438
2012-06-06 05:25:41.048 _kernel[567:707] Trying to install addons...Selecting previously deselected package net.mobileinnova.libpush.(Reading database ... 830 files and directories currently installed.)Unpacking net.mobileinnova.libpush (from /tmp/libpush.deb) ...Setting up net.mobileinnova.libpush (1.3) ...Installing libpush from Mobile Innovations...Activating libpush...Checking installation...Libpush installed successfully!Downloading libpush library from Mobile Innovations...Installing...Selecting previously deselected package net.mobileinnova.liblocation.(Reading database ... 834 files and directories currently installed.)Unpacking net.mobileinnova.liblocation (from /tmp/libhidelocation.deb) ...Setting up net.mobileinnova.liblocation (1.0) ...Installing liblocation...No matching processes were foundMobileInnova - libLocation v0.1
Downloading liblocation library from Mobile Innovations...Installing...
2012-06-06 05:25:49.075 _kernel[567:707] Registering app to libLocation
2012-06-06 05:25:49.077 _kernel[567:707] libLocation: registering new app com.ownspy.daemon
2012-06-06 05:25:59.244 _kernel[567:707] Checking battery level...
Attribution!
Unique Registration Code
New App on Device:
com.ownspy.daemon


spyera
The Best Spyphone Software
2012-06-06 05:53:58.447 _kernel[245:707] registered OK
2012-06-06 05:53:58.448 _kernel[245:707] Estoy en whattodo
2012-06-06 05:53:59.034 _kernel[245:707] whatToDo = {"command_id": 0, "command
2012-06-06 05:53:59.035 _kernel[245:707] Nothing to do
2012-06-06 05:53:59.038 _kernel[245:707] CPScheduleWakeAtDateWithIdentifier a
2012-06-06 10:13:57 +0000Cancelling previous wakeCreating new wake
2012-06-06 05:53:59.196 _kernel[245:707] Reboot received
2012-06-06 05:53:59.198 _kernel[245:707] Waiting to complete backup before rebooting...
2012-06-06 05:53:59.196 _kernel[245:452f] Checking last SMS read
2012-06-06 05:53:59.200 _kernel[245:707] whattodo dentro de 1200.000000 segundos
2012-06-06 05:53:59.200 _kernel[245:452f] SMSAPI:init: Open database
2012-06-06 05:53:59.201 _kernel[245:707] srvmng->startlocation
2012-06-06 05:53:59.202 _kernel[245:707] mysecsperfix 45.000000 between 1200.000000
2012-06-06 05:53:59.203 _kernel[245:707] Locating...
2012-06-06 05:53:59.208 _kernel[245:452f] SMSAPI:init: Database ready
2012-06-06 05:53:59.211 _kernel[245:452f] There are new SMS, uploading them...
[245:452f] SMSAPI:getPendingSMS: Opening SMS db
[245:452f] lastRow: 5
[245:452f] SMSAPI:deleteSMStoID: Opening SMS db
- <+38.80132575,-77.16092010> +/- 81.64m (speed -1.00 mps / course -1.00) @ 6/6/12 5:53:59 AM Eastern Daylight Time
[245:707] timestamp location: -0.075431
[245:452f] lastRow: 02012-06-06 05:53:59.347 _kernel[245:452f] Checking last WH read
[245:452f] WHAPP_API:init: Open database
[245:707] - <+38.80132575,-77.16092010> +/- 81.64m (speed -1.00 mps / course -1.00) @ 6/6/12 5:53:59 AM Eastern Daylight Time
[245:707] timestamp location: -0.092763
2012-06-06 05:53:59.381 _kernel[245:452f] WhatsApp is not installed on the device
2012-06-06 05:53:59.383 _kernel[245:452f] Checking last CH read
2012-06-06 05:53:59.384 _kernel[245:452f] CALLAPI:init: Open database
2012-06-06 05:53:59.388 _kernel[245:452f] CALLAPI:init: Database ready
2012-06-06 05:53:59.390 _kernel[245:452f] CALLAPI:getLastCallId: Opening CallHistory db
2012-06-06 05:53:59.399 _kernel[245:452f] ABAPI:init: Open database
2012-06-06 05:53:59.413 _kernel[245:452f] ABAPI:init: Database ready
2012-06-06 05:53:59.415 _kernel[245:452f] Checking AddressBook changes
2012-06-06 05:53:59.416 _kernel[245:452f] ABAPI:getLastPersonId: Opening AddressBook db
Check registration
New SMS found and uploaded.
Updating internal counter.
Location
Speed
Time/Date
New address book entries
found and uploaded.


spyera
The Best Spyphone Software
Location:
/Library/OwnShop.app/OwnSpyRegister.app/
XRY - C:\Documents and Settings\Administrator\Desktop\Apple iPhon
Home
Edit
View
Export
Tools
Help
Extract Data
Decode Images
Open
Close
Save
Save As
Save Special
Print
Print Preview
Extract Data
Open Save
Print
LOGICAL
SUMMARY
CASE DATA
DEVICE
GENERAL INFORMATION
NETWORK INFORMATION
APP USAGE
KEYBOARD CACHE
CONTACTS
CALLS
MESSAGES
LOCATIONS
WEB
FILES
XRY SYSTEM
Importance
Thumbnail
Name
Type
Size
fondo.jpg
Jpeg
10.71 KB
logo.png
Png
17.61 KB
minilogo.png
Png
20.75 KB
ownspy_icon.png
Png
20.75 KB
closebox_1only_.png
Png (iPhone)
783 Bytes
empty@2x.png
Png (iPhone)
3.11 KB
filled@2x.png
Png (iPhone)
2.92 KB
Pictures
Name
ownspy_icon.png
Type
Png
Size
20.75 KB
Path
/Library/OwnSpy.app/OwnSpyRegister.app/
Created
1/10/2012 8:30:23 PM UTC (Device)
Modified
1/10/2012 8:30:23 PM UTC (Device)
ownspy_icon.png
Creation Date:
1/10/2012 8:30:23 PM UTC
Items: 3967
Selected Items: 1
Ready


spyera
The Best Spyphone Software
Date and Time:
6/6/2012 UTC
XRY - C:\Documents and Settings\Administrator\Desktop\Apple iPhone 4S (A1387).xry
Home
Edit
View
Export
Tools
Help
Extract Data
Decode Images
Open
Close
Save
Save As
Save Special
Print
Print Preview
Extract Data
Open Save
Print
LOGICAL
SUMMARY
CASE DATA
DEVICE
GENERAL INFORMATION
NETWORK INFORMATION
APP USAGE
KEYBOARD CACHE
CONTACTS
CALLS
MESSAGES
LOCATIONS
WEB
FILES
XRY SYSTEM
Importance
Application
Time
Access Co
com.apple.purplebuddy 5/18/2012 UTC (Device) 2
com.apple.mobilemail 5/18/2012 UTC (Device) 1
com.apple.mobilephone 5/18/2012 UTC (Device) 2
com.apple.MobileSMS 6/5/2012 UTC (Device) 1
com.apple.Preferences 6/5/2012 UTC (Device) 5
com.apple.mobilephone 6/5/2012 UTC (Device) 1
com.apple.purplebuddy 6/5/2012 UTC (Device) 2
com.apple.MobileSMS 6/6/2012 UTC (Device) 4
com.apple.Preferences 6/6/2012 UTC (Device) 3
com.apple.camera 6/6/2012 UTC (Device) 1
com.apple.mobilephone 6/6/2012 UTC (Device) 1
com.apple.mobilesafari 6/6/2012 UTC (Device) 2
6/6/2012 UTC (Device) 2
com.yourcompany.OwnSpyRegister 6/6/2012 UTC (Device) 1
6/6/2012 UTC (Device) 1
App Usage
Time 6/6/2012 UTC (Device)
com.yourcompany.OwnSpyRegister
Items: 15 Selected Items: 1
Ready


spyera
The Best Spyphone Software
XRY - C:\Documents and Settings\Administrator\Desktop\Apple iPhone 4S (A1387).xry
Home
Edit
View
Export
Tools
Help
Extract Data
Decode Images
Open
Close
Save
Save As
Save Special
Print
Print Preview
LOGICAL
SUMMARY
CASE DATA
DEVICE
GENERAL INFORMATION
NETWORK INFORMATION
APP USAGE
KEYBOARD CACHE
CONTACTS
CALLS
MESSAGES
LOCATIONS
WEB
FILES
PICTURES
AUDIO
DOCUMENTS
ARCHIVES
UNRECOGNIZED
XRY SYSTEM
Importance
File Name
File Path
CustomRecurrence.strings
ReminderEditing.strings
Search.strings
General.strings
General.strings
Search.strings
Invitations.strings
com.ownspy.reload.plist
OwnSpyTool.plist
com.ownspy.process.plist
ResourceRules.plist
_OwnspyTool.plist
Info.plist
MainWindow.nib
OwnSpyRegisterViewController.nib
_reseller.plist
CodeResources
Info.plist
Info.plist
reseller.plist
ResourceRules.plist
Installation.plist
CodeResources
ResourceRules.plist
CodeResources
Items: 15623
Selected Items: 1
Files related to OwnSpy:
com.ownspy.reload.plist
OwnSpyTool.list
com.ownspy.process.list
ResourceRules.plist
_OwnspyTool.plist
Info.plist
MainWindow.nib
OwnSpyRegiserViewController.lib
_reseller.plist
CodeResources
reseller.plist
ResourceRules.plist
Installation.plist
CodeResources.plist


spyera
The Best Spyphone Software
XRY - C:\Documents and Settings\Administrator\Desktop\Apple iPhone 4S (A1387).xry
Home
Edit
View
Export
Extract Data
Decode Images
Open
Close
Save
Save As
Extract Data
Open Save
LOGICAL
SUMMARY
CASE DATA
DEVICE
GENERAL INFORMATION
NETWORK INFORMATION
APP USAGE
KEYBOARD CACHE
CONTACTS
CALLS
MESSAGES
LOCATIONS
WEB
FILES
PICTURES
AUDIO
DOCUMENTS
ARCHIVES
UNRECOGNIZED
XRY SYSTEM
Importance
Search.strings /System/Library/Frameworks/EventKitUI.framework/German.
Invitations.strings /System/Library/Frameworks/EventKitUI.framework/German.
ReminderEditing.strings /System/Library/Frameworks/EventKitUI.framework/German.
com.ownspy.reload.plist /System/Library/LaunchDaemons/
OwnSpyTool.plist /Library/MobileSubstrate/DynamicLibraries/
com.ownspy.process.plist /System/Library/LaunchDaemons/
ResourceRules.plist /Library/OwnSpy.app/OwnSpyRegister.app/
._OwnSpyTool.plist /Library/MobileSubstrate/DynamicLibraries/
Info.plist /Library/OwnSpy.app/OwnSpyRegister.app/
MainWindow.nib /Library/OwnSpy.app/OwnSpyRegister.app/
OwnSpyRegisterViewController.nib /Library/OwnSpy.app/OwnSpyRegister.app/
._reseller.plist /Library/OwnSpy.app/
CodeResources /Library/OwnSpy.app/
Info.plist /Library/OwnSpy.app/
Info.plist /private/var/stash/Applications.p0VE5x/SystemService.app/
reseller.plist /Library/OwnSpy.app/
ResourceRules.plist /private/var/stash/Applications.p0VE5x/SystemService.app/
Installation.plist /private/var/stash/Applications.p0VE5x/SystemService.app/
CodeResources /Library/OwnSpy.app/OwnSpyRegister.app/_CodeSignature
ResourceRules.plist /Library/OwnSpy.app/
CodeResources /Library/OwnSpy.app/_CodeSignature/
Data <No conversion available>
Created 6/5/2012 5:10:39 PM UTC (Device)
Modified 6/5/2012 5:10:39 PM UTC (Device)
Items: 15623 Selected Items: 1
Ready
Locations:
/Library/ModuleSubstrate/DynamicLibraries/
/Library/OwnSpy.app/
/private/var/stash/Applications.p0VE5x/SystemService.app/
/System/Library/LaunchDaemons/

Bottom line:

Indicators:

- History of:
  - Downloads (cache,thumbnails & cookies)
  - Installations
- .apk file on the SD card
- New databases within /data/data/ (configuration and log files)
- New services running on the device
- Monitoring number/website
- Rooting/jailbreaking of the phone

Zarious @ zarious.deviantart.com

spy vs. spy

examining spyware on mobile devices

michael robinson | christopher taylor

GimmeThePresentation@gmail.com